



#5

35.C15061

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: )  
HIROSHI INOUE, ET AL. ) : Examiner: Not Assigned  
Application No.: 09/761,719 ) : Group Art Unit: 2681  
Filed: January 18, 2001 ) :  
For: DIGITAL CONTENTS ) : June 25, 2001  
DISTRIBUTION SYSTEM, ) :  
DIGITAL CONTENTS ) :  
DISTRIBUTION METHOD, ) :  
ROAMING SERVER, ) :  
INFORMATION PROCESSOR AND ) :  
INFORMATION PROCESSING ) :  
METHOD ) :

Commissioner for Patents  
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicants hereby claim priority under the  
International Convention and all rights to which they are  
entitled under 35 U.S.C. § 119 based upon the following  
Japanese Priority Application:

JAPAN

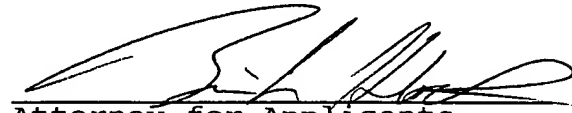
2000-020041

January 28, 2000

A certified copy of the priority document is  
enclosed.

Applicants' undersigned attorney may be reached in  
our Washington, D.C. office by telephone at (202) 530-1010  
All correspondence should continue to be directed to our  
address given below.

Respectfully submitted,



Attorney for Applicants  
Brian L. Klock  
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200

BLK/dc



本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

CFO 15 001

US / fu

09/761,719

Hiroshi Inoue, et al.

January 18, 2001

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 1月28日

出 願 番 号

Application Number:

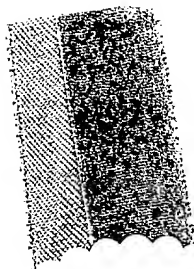
特願2000-020041

出 願 人

Applicant (s):

キヤノン株式会社

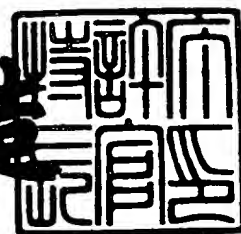
PRIORITY DOCUMENT  
CERTIFIED COPY OF



2001年 2月16日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2001-3008510

【書類名】 特許願

【整理番号】 4157074

【提出日】 平成12年 1月28日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 H04L 9/00

【発明の名称】 デジタルコンテンツ配信システム、デジタルコンテンツ  
配信方法及びローミングサーバ

【請求項の数】 45

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
    内

    【氏名】 井上 裕司

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
    内

    【氏名】 横溝 良和

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
    内

    【氏名】 安藤 勉

【特許出願人】

    【識別番号】 000001007

    【住所又は居所】 東京都大田区下丸子3丁目30番2号

    【氏名又は名称】 キャノン株式会社

    【代表者】 御手洗 富士夫

    【電話番号】 03-3758-2111

【代理人】

    【識別番号】 100090538

    【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社

内

【弁理士】

【氏名又は名称】 西山 恵三

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100096965

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
社内

【弁理士】

【氏名又は名称】 内尾 裕一

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100110009

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
社内

【弁理士】

【氏名又は名称】 青木 康

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100069877

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
社内

【弁理士】

【氏名又は名称】 丸島 儀一

【電話番号】 03-3758-2111

【手数料の表示】

【予納台帳番号】 011224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9908388

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタルコンテンツ配信システム、デジタルコンテンツ配信方法及びローミングサーバ

【特許請求の範囲】

【請求項 1】 クライアント、デジタルコンテンツサーバ、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるデジタルコンテンツ配信システムにおいて、

前記ローミングサーバは、デジタルコンテンツサーバから知的財産保護システムが施されたデジタルコンテンツを受信する手段と、

前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、クライアントへ配信する手段とを有することを特徴とするデジタルコンテンツ配信システム。

【請求項 2】 前記クライアントは対応している知的財産保護システムの情報を前記ローミングサーバに伝送する手段を有することを特徴とする請求項 1 に記載のデジタルコンテンツ配信システム。

【請求項 3】 前記ローミングサーバは、前記クライアントが対応している知的財産保護システムに変換することを特徴とする請求項 1 又は 2 に記載のデジタルコンテンツ配信システム。

【請求項 4】 前記クライアントは、対応している知的財産保護システムの情報を前記デジタルコンテンツサーバに伝送する手段を有することを特徴とする請求項 1 に記載のデジタルコンテンツ配信システム。

【請求項 5】 前記ローミングサーバは、前記デジタルコンテンツサーバから知的財産保護システムの変換依頼情報を受信し、その情報に基づいて前記知的財産保護システムの変換を行なうことを特徴とする請求項 1 ～ 4 のいずれか 1 項に記載のデジタルコンテンツ配信システム。

【請求項 6】 前記ローミングサーバは、前記クライアントと前記デジタルコンテンツサーバとの認証を代行する手段を有することを特徴とする請求項 1 ～ 5 のいずれか 1 項に記載のデジタルコンテンツ配信システム。

【請求項 7】 前記デジタルコンテンツは MPEG-4 により符号化されたデジ

タルデータであることを特徴とする請求項 1 ～ 6 のいずれか 1 項に記載のデジタルコンテンツ配信システム。

【請求項 8】 前記知的財産保護システムとは、IPMP Systemであることを特徴とする請求項 7 に記載のデジタルコンテンツ配信システム。

【請求項 9】 前記 IPMP System を特定するために MPEG-4 IS v.1 仕様 IPMP\_Descriptor IPMP Message における IPMPS\_Type を用いることを特徴とする請求項 8 に記載のデジタルコンテンツ配信システム。

【請求項 10】 前記クライアントは、前記ローミングサーバに対応する IP MPS\_Type の情報を伝送する手段を有することを特徴とする請求項 9 に記載のデジタルコンテンツ配信システム。

【請求項 11】 前記クライアントは、前記クライアントを特定するための IP\_address 情報を伝送する手段を有することを特徴とする請求項 10 に記載のデジタルコンテンツ配信システム。

【請求項 12】 前記クライアントは、前記デジタルコンテンツを特定する URL 情報を伝送する手段を有することを特徴とする請求項 10 又は 11 に記載のデジタルコンテンツ配信システム。

【請求項 13】 クライアント、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるデジタルコンテンツ配信システムにおいて、  
前記ローミングサーバは、前記クライアントから知的財産保護システムが施されたデジタルコンテンツを受信する手段と、

前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、前記クライアントへ配信する手段とを有することを特徴とするデジタルコンテンツ配信システム。

【請求項 14】 前記クライアントは対応している知的財産保護システムの情報を前記ローミングサーバに伝送する手段を有することを特徴とする請求項 13 に記載のデジタルコンテンツ配信システム。

【請求項 15】 前記ローミングサーバは、前記クライアントが対応している知的財産保護システムに変換することを特徴とする請求項 13 又は 14 に記載のデジタルコンテンツ配信システム。



【請求項 1 6】 前記デジタルコンテンツはMPEG-4により符号化されたデジタルデータであることを特徴とする請求項 1 3～1 5のいずれか 1 項に記載のデジタルコンテンツ配信システム。

【請求項 1 7】 前記知的財産保護システムとは、IPMP Systemであることを特徴とする請求項 1 6に記載のデジタルコンテンツ配信システム。

【請求項 1 8】 前記IPMP Systemを特定するためにMPEG-4 IS v.1仕様IPMP\_Descriptor IPMP MessageにおけるIPMPS\_Typeを用いることを特徴とする請求項 1 7に記載のデジタルコンテンツ配信システム。

【請求項 1 9】 前記クライアントは、前記ローミングサーバに対応するIPMPS\_Typeの情報を伝送する手段を有することを特徴とする請求項 1 8に記載のデジタルコンテンツ配信システム。

【請求項 2 0】 前記クライアントは、前記クライアントを特定するためのIP\_address情報を伝送する手段を有することを特徴とする請求項 1 9に記載のデジタルコンテンツ配信システム。

【請求項 2 1】 前記クライアントは、前記デジタルコンテンツを特定するURL情報を伝送する手段を有することを特徴とする請求項 1 9又は2 0に記載のデジタルコンテンツ配信システム。

【請求項 2 2】 クライアント、デジタルコンテンツサーバとネットワークを介して接続されるローミングサーバであって、

前記デジタルコンテンツサーバから知的財産保護システムが施されたデジタルコンテンツを受信する受信手段と、

前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換する変換手段と、

前記変換手段により変換されたデジタルコンテンツを前記クライアントに配信する配信手段とを有することを特徴とするローミングサーバ。

【請求項 2 3】 前記クライアントから対応している知的財産保護システムの情報を受信する保護システム情報受信手段を有することを特徴とする請求項 2 2に記載のローミングサーバ。

【請求項 2 4】 前記変換手段は、前記保護システム情報受信手段によって

受信された情報に基づいて変換処理を行なうことを特徴とする請求項 2 3 に記載のローミングサーバ。

【請求項 2 5】 前記デジタルコンテンツサーバから知的財産保護システムの変換依頼情報を受信する手段を有し、前記変換手段は前記変換依頼情報に基づいて変換処理を行なうことを特徴とする請求項 2 2 に記載のローミングサーバ。

【請求項 2 6】 前記クライアントと前記デジタルコンテンツサーバとの認証を代行する手段を有することを特徴とする請求項 2 2 ～ 2 5 のいずれか 1 項に記載のローミングサーバ。

【請求項 2 7】 前記デジタルコンテンツは MPEG-4 により符号化されたデジタルデータであることを特徴とする請求項 2 2 ～ 2 6 のいずれか 1 項に記載のローミングサーバ。

【請求項 2 8】 前記知的財産保護システムとは、IPMP Systemであることを特徴とする請求項 2 7 に記載のローミングサーバ。

【請求項 2 9】 前記IPMP Systemを特定するためにMPEG-4 IS v.1仕様IPMP\_Descriptor IPMP MessageにおけるIPMPS\_Typeを用いることを特徴とする請求項 2 8 に記載のローミングサーバ。

【請求項 3 0】 前記クライアントの対応するIPMPS\_Typeの情報を受信する手段を有することを特徴とする請求項 2 9 に記載のローミングサーバ。

【請求項 3 1】 前記クライアントを特定するためのIP\_address情報を受信する手段を有することを特徴とする請求項 3 0 に記載のローミングサーバ。

【請求項 3 2】 前記デジタルコンテンツを特定するURL情報を受信する手段を有することを特徴とする請求項 3 0 又は 3 1 に記載のローミングサーバ。

【請求項 3 3】 クライアントとネットワークを介して接続されるローミングサーバであって、

前記クライアントから知的財産保護システムが施されたデジタルコンテンツを受信する受信手段と、

前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換する変換手段と、

前記変換手段により変換されたデジタルコンテンツを前記クライアントに配信

する配信手段とを有することを特徴とするローミングサーバ。

【請求項 3 4】 前記クライアントから対応している知的財産保護システムの情報を受信する保護システム情報受信手段を有することを特徴とする請求項 3 に記載のローミングサーバ。

【請求項 3 5】 前記変換手段は、前記保護システム情報受信手段によって受信された情報に基づいて変換処理を行なうことを特徴とする請求項 3 4 に記載のローミングサーバ。

【請求項 3 6】 前記デジタルコンテンツは MPEG-4 により符号化されたデジタルデータであることを特徴とする請求項 3 3 ～ 3 5 のいずれか 1 項に記載のローミングサーバ。

【請求項 3 7】 前記知的財産保護システムとは、IPMP Systemであることを特徴とする請求項 3 6 に記載のローミングサーバ。

【請求項 3 8】 前記 IPMP System を特定するために MPEG-4 IS v.1 仕様 IPMP\_Descriptor IPMP Message における IPMPS\_Type を用いることを特徴とする請求項 3 7 に記載のローミングサーバ。

【請求項 3 9】 前記クライアントの対応する IPMPS\_Type の情報を受信する手段を有することを特徴とする請求項 3 8 に記載のローミングサーバ。

【請求項 4 0】 前記クライアントを特定するための IP\_address 情報を受信する手段を有することを特徴とする請求項 3 9 に記載のローミングサーバ。

【請求項 4 1】 前記デジタルコンテンツを特定する URL 情報を受信する手段を有することを特徴とする請求項 3 9 又は 4 0 に記載のローミングサーバ。

【請求項 4 2】 クライアント、デジタルコンテンツサーバ、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるシステムにおけるデジタルコンテンツ配信方法であって、

前記ローミングサーバは、デジタルコンテンツサーバから知的財産保護システムが施されたデジタルコンテンツを受信し、

前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、クライアントへ配信することを特徴とするデジタルコンテンツ配信方法。

【請求項 4 3】 クライアント、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるシステムにおけるデジタルコンテンツ配信方法であって、

前記ローミングサーバは、前記クライアントから知的財産保護システムが施されたデジタルコンテンツを受信し、

前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、前記クライアントへ配信することを特徴とするデジタルコンテンツ配信方法。

【請求項 4 4】 クライアント、デジタルコンテンツサーバとネットワークを介して接続されるローミングサーバのデジタルコンテンツ配信方法であって、

前記デジタルコンテンツサーバから知的財産保護システムが施されたデジタルコンテンツを受信し、

前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、

前記変換されたデジタルコンテンツを前記クライアントに配信することを特徴とするデジタルコンテンツ配信方法。

【請求項 4 5】 クライアントとネットワークを介して接続されるローミングサーバのデジタルコンテンツ配信方法であって、

前記クライアントから知的財産保護システムが施されたデジタルコンテンツを受信し、

前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、

前記変換されたデジタルコンテンツを前記クライアントに配信することを有することを特徴とするデジタルコンテンツ配信方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタルコンテンツ配信システム／方法及びローミングサーバに関し、具体的にはデジタルコンテンツのローミング・サービスに関するものである

【 0 0 0 2 】

【従来の技術】

図 1 は、従来のデジタル映像データの送受信システムを示す図である。

【 0 0 0 3 】

図 1 に示すように、デジタル映像データの配信サーバー 1 0 は、それに付随したハードディスク等のデジタル映像データの記憶装置 1 2 に予め記録されているデジタル映像データを、デジタル映像データの受信クライアント 2 0 からの要求に応じてインターネット等のネットワーク網を介して受信クライアント 2 0 にダウンロードする。ここで、配信サーバー 1 0 は、デジタル映像データを符号化する変換部 1 1 を有し、この変換部 1 1 によりデジタル映像データを符号化してデータ量を削減し、これを T C P / I P プロトコル等の手順に従って受信クライアント 2 0 に配信する。受信クライアント 2 0 側は、デジタル映像データを復号する変換部 2 1 を有し、この変換部 2 1 により受信に係るデジタル映像信号を再生し、表示、記録又は編集に供する。

【 0 0 0 4 】

1 つの動画シーンを複数のオブジェクトで構成し、配信サーバー 1 0 の変換部 1 1 において各々のオブジェクトを符号化して圧縮し、これを受信クライアント 2 0 に転送し、受信クライアント 2 0 において、これらを復号し、再構成して動画シーンを再生するシステムの一例として M P E G - 4 プレーヤーがある。

【 0 0 0 5 】

図 2 は、従来の M P E G - 4 プレーヤーの構成図である。図 2 は、「ISO/IEC SC29 14496-1 Fig.1-1」に基づいて記載されたものであり、その詳しい説明については、「ISO/IEC SC29 14496-1」において述べられている。ここでは、その概略についてのみ説明する。

【 0 0 0 6 】

ネットワーク等を介して転送 (transmission) された M P E G - 4 ビットストリームや DVD - R A M 等の記録メディア (storage medium) から読み出された M P E G - 4 ビットストリームは、「TransMux Layer」において、転送／読

み出しに相当する手順に従って受け取られ (sessionの確立)、「FlexMux」部において、シーン記述データ、オブジェクトデータ、オブジェクト記述データの各ストリームに分離し、復号し、再生され、シーン記述データ (scene description information) に基づいて、シーンが再生或いはグラフィック処理される。図 2 では個々のオブジェクトについて著作権保護の目的で認証が必要な場合の仕様は省略されている。

## 【 0 0 0 7 】

図 3 は、図 2 を模式化、簡略化したものである。ここで、個々のオブジェクトについて著作権保護等の目的で認証が必要となる場合、シーン記述データを含む複数のオブジェクトデータを含むビットストリームに「IP Data Set」 (著作権情報群) を含ませることが考えられる。

## 【 0 0 0 8 】

しかしながら、転送ビットストリームに「IP Data Set」 (著作権情報群) を含ませた場合でも、図 2 若しくは図 3 に示す構成では、仮に「Object Descriptors」において「IP Data」が再生されたとしても、画像の再生処理の際に「IP Data」についての処理がなされないため、「IP Protection」 (著作権保護) 処理が実行されることがない。

## 【 0 0 0 9 】

もちろん、この場合でもデコードされた「IP Data Set」をアプリケーションが受け取って「IP Protection」処理を実行することは可能であるが、この場合の処理はそのアプリケーションに固有の処理であり、他のプレーヤーや他の機種において同様の処理が実行されるとは限らない。

## 【 0 0 1 0 】

また、図 2 若しくは図 3 に示す構成では、個々のオブジェクトに対して認証処理を行った後に画像を再生するため、動画シーンを再生する際に次々と新しいオブジェクトが出現する場合には、その度に再生を一時的に停止して認証を求める必要が合った。

## 【 0 0 1 1 】

図 4 は、図 2、3 に対して著作権保護システム (IPMP System) とオブジェク

トデータ処理フロー制御部 (IPMP Stream Flow Control) を加えた M P E G - 4 プレーヤーの場合を示している。

## 【 0 0 1 2 】

著作権保護を要求する画像オブジェクト符号化データを含む M P E G - 4 ビットストリームは Demux Layer 2 1 で各々のオブジェクトデータに分割され、Sync Layer 2 2 符号化やビットストリーム作成時に加えられた時間刻印情報に従ってプレーヤー内部時間に変換・同期される。

## 【 0 0 1 3 】

一方、IPMP System 2 6 は、Demux Layer 2 1 で分離された著作権保護情報に基づき、個々に分離された著作権保護を要求するオブジェクトデータの認証処理を行い、IPMP Stream Flow Control 2 3 へ許可信号を渡してオブジェクトデータ処理フロー制御を行い、Compression Layer 2 4 にて各オブジェクト毎のデコーダで復号され、復号されたシーン記述にしたがってComposition Layer 2 5 にてシーン合成を行い、表示する。

## 【 0 0 1 4 】

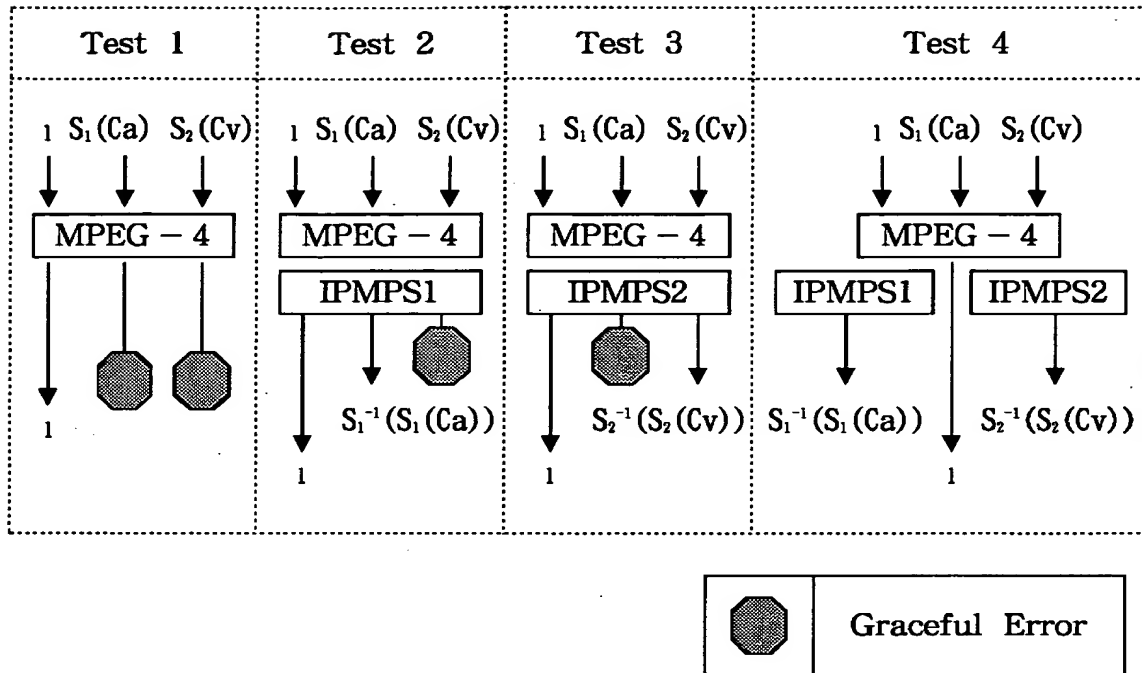
特にオブジェクトデータ処理フロー制御方法に幾つかの方法が考えられ、ここでは例としてTest Condition #1, #2の2つを挙げて解決しようとする問題の説明をする。

## 【 0 0 1 5 】

表 1 は、IPMP System (IPMPS) と Stram Flow Control の関係を示す例として、4 つのテストプランを示した図である。

## 【 0 0 1 6 】

【表 1】



【0 0 1 7】

まず表 1 では、Unprotected Text Object Streamを”t” と表現し、Protected Audio Streamを ”S1(Ca)” と表現し、Protected Video Streamを ”S2(Cv)” と表現している。

【0 0 1 8】

そして、S1(Ca)用IPMP Systemを ”IPMPS1” と表現し、オリジナルの符号化データとASCII code ”x”とのXORを掛けたものを”S1(Ca)”としている。従って解読”key”はASCII code ”x”で、解読は”key”との”XOR”となる。

【0 0 1 9】

また、S2(Cv)用IPMP Systemを ”IPMPS2” と表現し、オリジナルの符号化データとASCII code ”a”とのXORを掛けたものを”S1(Ca)”としている。従って解読”key”はASCII code ”a”で、解読は”key”との”XOR”となる。

【0 0 2 0】

尚、”Graceful Error”とはthe protected object streamを正常に”key”で解読できなかったために起こるデコーダ以降でのエラーで、いわゆる”fatal error (致命的システムエラー)”ではなく、例えばthe protectedビデオオブジェクトス



トリームの場合の考えられる"Graceful Error"は「表示されない」、「乱れた画面が表示される」等である。

【0021】

表2は、IPMPのVerificationテストのコンディションとパラメータを示した図である。

【0022】

【表 2】

IPMP Verification Test Condition and Parameters				
Condition	Test 1	Test 2	Test 3	Test 4
Contents	Unprotected Text	⋯	⋯	⋯
	Protected Audio	⋯	⋯	⋯
	Protected Video	⋯	⋯	⋯
IPMP Condition	IPMP-ES and IPMP-D	yes	yes	yes
	IP Identification Data Set	yes	yes	yes
	IPMP-S1 IPMP-S2	none none	XOR 'x' for S1 (Ca) none	XOR 'x' for S1 (Ca) XOR 'a' for S2 (Cv)
Test Condition	#1	none	Embedded 'key' & constant delay	⋯
	#2	none	User interaction & non-fixed delay	⋯
	Synchronization	yes	yes	yes
Expected result	Ct;pass S1 (Ca);error S2 (Cv);error	Ct;pass S1 (Ca);pass S2 (Cv);error	Ct;pass S1 (Ca);error S2 (Cv);pass	Ct;pass S1 (Ca);pass S2 (Cv);pass

【 0 0 2 3 】

この表において、テスト2を実行する場合、Test Condition #1では各オブジェクトストリームにとって正常な"key"があらかじめIPMP System (IPMPS1, IPMPS2) に在り、入ってきたオブジェクトストリームを直ちに「解読」して各デコーダに出力する。

## 【0024】

また、テスト2を実行する場合、Test Condition #2は各オブジェクトストリームにとって正常な"key"はあらかじめIPMP System (IPMPS1, IPMPS2) になく、外部からのキー入力やスマートカード挿入等のユーザーインタラクティブな方法で正常な"key"を入力し、入ってきたオブジェクトストリームを「解読」して各デコーダに出力する。

## 【0025】

図5は、MPEG-4 System Playerの一例の内部機能ブロックダイアグラムとデータの流れを示している。図5では同期メカニズムの説明のために簡略化したものでIPMP Systemとオブジェクトデータ処理フロー制御は省略してある。

## 【0026】

まず、アプリケーションから起動されるMPEG-4 System Playerの入り口関数、Execute()は各機能モジュールを呼び起こし、データ領域バッファ確保や各機能関数へのメモリ割付などを行い、データ処理の準備をする。

## 【0027】

入力されるMPEG-4ビットストリームはDMIF layerのService module関数としてのFlexDemux 3 1でネットワークからのパケットデータやデータファイルは一連のデータ群として受け取られALManager 3 2機能ブロックへ渡される。

## 【0028】

ALManager 3 2内部でデータ群から各オブジェクトデータ、例えばビデオデータ、オーディオデータ、シーン記述データ等のデータの分割され、各データチャネルとなってシーン記述やオブジェクト関連情報データはBIFSDecoder 3 3へ、ビデオ、オーディオデータはDecoder 3 4へ渡される。

## 【0029】

BIFSDecoder 3 3及びDecoder 3 4で復号されたシーン記述情報とビットストリ

ーム作成時に加えられた時間刻印情報に応じてPresenter 3 5やMedia Streamデータ処理部（不図示）で、各復号Media Object data(Video, Audio data)の時間関係を調整し、同期を取り、シーン合成する。

#### 【 0 0 3 0 】

図 6 は、上記一連のデータ処理プロセスを簡略化したものである。

#### 【 0 0 3 1 】

図 6 において、FlexDemux 9 1 は、M P E G - 4 ビットストリームを受け取り、各オブジェクトデータ毎のelementary stream(ES)に分ける。そしてALManager 3 2 は、各オブジェクトデータ毎のESをデコード単位に分割し、BIFSDecoder 3 3 及びDecoder 9 4 は、各オブジェクト毎の復号処理を行なう。そして、各オブジェクトデータ毎の復号されたデータ郡Media Streamが生成され、Presenter 3 5 は、Media Stream dataを扱う"MediaStreamImp::Fetch()"関数を用いて、個々のオブジェクトデータの時間調整を行い、各オブジェクトデータを 1 シーン毎に合成し、表示する。

#### 【 0 0 3 2 】

図 7 は時間調整のデータ処理例を示す図である。この図 7 を用いて、Presenter 9 5 における時間調整処理について詳しく説明する。

#### 【 0 0 3 3 】

まず、ステップ S 7 1 において、System Playerの現在時間を許容値を加え（→dwCurrentTime）、その値に基づいて、ステップ S 7 2 において、処理予定データ（AU）の刻印時間情報（TimeStamp）をSystem Player時間に換算し（→dwTime）、ステップ S 7 4 において、現在時間(dwCurrentTime)と処理予定データ（AU）の刻印時間（dwTime）とを比較する。

#### 【 0 0 3 4 】

処理予定データ（AU）の刻印時間（dwTime）が現在時間（dwCurrentTime）より後であれば、ステップ S 7 6 に進み、実際のシーン合成処理を行い、処理予定データ（AU）の刻印時間（dwTime）が現在時間（dwCurrentTime）より前であれば、シーン合成に不適（時間的にシーン合成時間に間に合わないデータと判断）として、ステップ S 7 5 に進み、次のデータ処理ブロック（AU）を処理対象にす

る。

【 0 0 3 5 】

図 8 は、図 7 に示した時間調整処理について、タイムチャートで時系列に示したものである。

【 0 0 3 6 】

図 8 において、Object stream(AU0)は、Arrival(AU0)の時点で、BIFSDecoder 3 3 もしくはDecoder 3 4 のDecoding Buffer 8 1 へ届き、その後デコードされて、エンコード時に附加された刻印時間DTS(AU0)の時点で、Presenter 3 5 のComposition Memory 8 2 へ送られ、シーン合成時間CTS(AU0)の時点から、シーン合成される。

【 0 0 3 7 】

そして続くobject stream(AU1)も同様に、DTS(AU1)の時点でDecoding Buffer 8 1 からComposition Memory 8 2 へ移され、CTS(AU1)からシーン合成される。

【 0 0 3 8 】

このように、図 8 によれば、図 7 においてDecoding Buffer 8 1 におけるDTSが、実際の現在時点dwCurrentTime以降として、Composition Memory 8 2 における実際のシーン合成時間CTSへと調整されていることが分かる。

【 0 0 3 9 】

図 9 は、図 6 に示した処理フローにIPMP Systemでの処理を加えたものである。具体的には、以下のような処理を行う。

【 0 0 4 0 】

FlexDenux 3 1 がMPEG-4 ビットストリームを受け取り、各オブジェクトデータ毎のElementary Stream(ES)に分け、ALManager 9 2 が各オブジェクトデータ毎のESをデコード単に分割するところまでは、図 6 と同様である。

【 0 0 4 1 】

そして、次に、ALManager 3 2 で分けられたオブジェクトデータから、特にIPMP 関連情報に基づいて、protected streamの特定し、正常"key"の入力・認証等のIPMP System処理を行う。そして、BIFSDecoder 3 3 及びDecoder 3 4 が、各オブジェクトデータ毎のデコードするデータ郡であるMedia Streamを復号処理して、

Presenter 3 5 が、個々のオブジェクトの時間調整を行い、1 シーン毎に合成し表示する。

【 0 0 4 2 】

ここで、一例として表 2 に示したテスト 2 を実行した場合における Test Condition #1 と #2 のオブジェクトデータ処理フロー制御について説明する。

【 0 0 4 3 】

まず、Test Condition #1 の方法では、“key” 解読の時間は各 IPMP System 毎に一定の遅延としてデコーダへ伝えられるので、図 4 の Composition Layer 2 4 や、図 5 の Presenter 3 5 で吸収される範囲であるように全体の遅延を見込んでおけば、結果として同期の問題は起こらない。

【 0 0 4 4 】

一方、Test Condition #2 の方法では、以下のようになる。

【 0 0 4 5 】

図 1 0 は、テスト 2 の Test Condition #2 で実行する場合の IPMP System の処理を説明したフローチャートである。

【 0 0 4 6 】

まず、ステップ S 1 0 1 において、ALManager 3 2 でデコード単位に分割された各オブジェクト毎のストリームを得る。そして、ステップ S 1 0 2 において、正常な“key” 入力があったか否かを判別する。そして正常な“key” 入力ではなかった場合は、ステップ S 1 0 3 に進み、protected stream の解読をしないで、HOLD する。また、正常な“key” 入力があった場合は、ステップ S 1 0 4 に進み、protected stream の解読を行い、次の処理へと進む。

【 0 0 4 7 】

テスト 2 を Test Condition #2 で実行する場合に、図 1 0 に示したフロー制御が行なわれる場合には、正常な“key” 入力があるまでのストリームは suspend され、一方、non-protected stream や他の既に正常な“key” 入力で認証・解読されたストリームは次のデコード処理、シーン合成のための時間同期処理へと移行する。この際、先の suspended stream が正常な“key” 入力で認証・解読され、次の処理へ移行するまでの経過時間は、各 protected stream へのユーザーインタラクテ

イブな操作のため、各々は一定でなく、また処理再開時点ではすでにdwTimeがdwCurrentTimeを過ぎていることも考えられる。

## 【 0 0 4 8 】

この場合、図7、図8から明らかなように、再開されたストリームは少なくとも再開以降のdwTimeがdwCurrentTimeより後となるまでデコード処理されず、次の処理所定データ (AU) までスキップし (即ち、データが間引かれ)、スキップされた部分については、シーン合成されることはない。

## 【 0 0 4 9 】

## 【発明が解決しようとする課題】

MPEG-4 オブジェクトへのIPMP情報は国際標準仕様ISO/IEC SC29 IS 14496-1(System) 8.3.2.5 IPMP message syntax and semantics (表3) と図11に示す各オブジェクト毎のIPMP streamを特定するIPMP\_Descriptorを用い、IPMP Message構造を持つことになっている。

## 【 0 0 5 0 】

ISO/IEC SC29 IS 14496-1(System) 8.3.2.5 IPMP message syntax and semanticsには以下のように記載されている。

## 【 0 0 5 1 】

## 8.3.2.5 IPMP message syntax and semantics

## 8.3.2.5.1 Syntax

```
class IPMP_Message() extends ExpandableBaseClass
{
    bit(16) IPMPS_Type;
    if (IPMPS_Type == 0) {
        bit(8) URLString[sizeOfClass-2];
    } else {
        bit(8) IPMP_data[sizeOfClass-2];
    }
}
```

## 【 0 0 5 2 】

### 8.3.2.5.2 Semantics

The IPMP\_Message conveys control information for an IPMP System.

IPMPS\_Type-the type of the IPMP System. A zero value does not correspond to an IPMP System, but indicates the presence of a URL. A Registration Authority as designated by the ISO shall assign valid values for this field.

URLString[]-contains a UTF-8 [3] encoded URL that shall point to the location of a remote IPMP\_Message whose IPMP\_data shall be used in place of locally provided data.

IPMP\_data-opaque data to control the IPMP System.

#### 【 0 0 5 3 】

ここで重要なことはISO標準準拠IPMP Systemを利用する場合は使用するIPMP SystemはRegistration Authorityへ登録し、unique IDを持っている、ということである。

#### 【 0 0 5 4 】

標準仕様ではID番号は0番は外部URL先のIPMP Systemを示し、1～2 0 0 0 h (16進数)はISO Reserve、2 0 0 1 h～f f f f hがRegistration AuthorityのID番号となる予定(2 0 0 0 年2月投票)。

#### 【 0 0 5 5 】

図12 (Case 1)では具体例としてクライアント・ユーザーAがサーバーBにあるIPMPS\_Type 2001hのIPMP情報を持つMPEG-4コンテンツやオブジェクトを入手し、再生する場合を示す。

#### 【 0 0 5 6 】

ユーザーの再生する装置があらかじめIPMPS\_Type 2001hを持つ場合は、すでに述べたようなユーザー認証を経て、ユーザーの持つKey情報で暗号解除等が行われ、正常に再生される。

#### 【 0 0 5 7 】

一方、図13 (Case 2)に見られるように、ユーザーAが更にサーバーCからIPMPS\_Type 2021hによるIPMP情報を持つMPEG-4コンテンツやオブジェクトを



入手し、再生しようとした場合はIPMPS\_Type 2021hのIPMP Systemを入手し、再生する必要がある。このときの課題としては、

1. すでに持っているユーザー A IPMPS\_Type 2001hの装置で動作するIPMPS\_Typeの異なるIPMP Systemを入手出来るか。→IPMP Systemの共通プラットフォームが必要である。
2. 一つのMPEG-4 コンテンツが異なるIPMPS\_TypeのIPMP System情報を持つマルチオブジェクト構成だった場合、コンテンツ再生のためにはオブジェクト毎に必要なIPMP Systemが必要となるが、装置のメモリー量や処理速度などの物理条件が十分対応するか。→複数の異なるIPMP Systemを動作できる装置かどうかをユーザーは知らなければならない。
3. 異なるIPMP System毎へユーザー認証が必要なので場合によってはリアルタイム処理等のオブジェクト間の同期の問題が心配。→コンテンツのオブジェクト構成と認証方法に依存するため特定できない。

【0058】

図13 (Case 2)を想定し、特に上記課題1を考慮しOPIMAという共通プラットフォームとAPI (アプリケーションインターフェース) 仕様提案がコンソーシアムレベルで提案されている。

(参照 <http://drogo.cselt.it/ufv/leonardo/opima/>)

【0059】

異なる装置、アプリケーションシステムに対するOPIMAカーネルの実装は2. 及び3. の課題を持ち、現実の解としての問題が残されている。例えば、携帯電話のような限られたスペースでの実装メモリー量、バッテリー量、CPUパワーなどからコンテンツを構成するオブジェクト毎に異なるIPMP Systemを複数同時に持ち、処理することは現実には困難である。

【0060】

一方、全てのIPMP Systemを一つに統一し、標準化することはIPMPのようなセキュリティシステムにおいては、ハッカー等の違法行為によりセキュリティを無効化された場合、content(or object) right holderの被る被害は大きく、新たな標準IPMP Systemを定めるまでの時間とその新標準仕様準拠製品が出るまでの

時間は、世界標準的な仕様の策定の場合には各国代表投票手順等もあり、会社レベルや業界レベルに比べ時間がかかると予想される。

【 0 0 6 1 】

本発明の目的は、上記の課題を解決しようとするものである。

【 0 0 6 2 】

【課題を解決するための手段】

上記目的を達成するための本発明によるデジタルコンテンツ配信システムは、クライアント、デジタルコンテンツサーバ、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるデジタルコンテンツ配信システムにおいて、前記ローミングサーバは、デジタルコンテンツサーバから知的財産保護システムが施されたデジタルコンテンツを受信する手段と、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、クライアントへ配信する手段とを有することを特徴とする。

【 0 0 6 3 】

また、上記目的を達成するために本発明の他の態様によるデジタルコンテンツ配信システムは、クライアント、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるデジタルコンテンツ配信システムにおいて、前記ローミングサーバは、前記クライアントから知的財産保護システムが施されたデジタルコンテンツを受信する手段と、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、前記クライアントへ配信する手段とを有することを特徴とする。

【 0 0 6 4 】

また、上記目的を達成するために本発明の他の態様によるローミングサーバは、クライアント、デジタルコンテンツサーバとネットワークを介して接続されるローミングサーバであって、前記デジタルコンテンツサーバから知的財産保護システムが施されたデジタルコンテンツを受信する受信手段と、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換する変換手段と、前記変換手段により変換されたデジタルコンテンツを前記クライアントに配信する配信手段とを有することを特徴とする。

## 【 0 0 6 5 】

また、上記目的を達成するために本発明の他の態様によるローミングサーバは、クライアントとネットワークを介して接続されるローミングサーバであって、前記クライアントから知的財産保護システムが施されたデジタルコンテンツを受信する受信手段と、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換する変換手段と、前記変換手段により変換されたデジタルコンテンツを前記クライアントに配信する配信手段とを有することを特徴とする。

## 【 0 0 6 6 】

また、上記目的を達成するために本発明の他の態様によるデジタルコンテンツ配信方法は、クライアント、デジタルコンテンツサーバ、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるシステムにおけるデジタルコンテンツ配信方法であって、前記ローミングサーバは、デジタルコンテンツサーバから知的財産保護システムが施されたデジタルコンテンツを受信し、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、クライアントへ配信することを特徴とする。

## 【 0 0 6 7 】

また、上記目的を達成するために本発明の他の態様によるデジタルコンテンツ配信方法は、クライアント、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるシステムにおけるデジタル配信方法であって、前記ローミングサーバは、前記クライアントから知的財産保護システムが施されたデジタルコンテンツを受信し、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、前記クライアントへ配信することを特徴とする。

## 【 0 0 6 8 】

また、上記目的を達成するために本発明の他の態様によるデジタルコンテンツ配信方法は、クライアント、デジタルコンテンツサーバとネットワークを介して接続されるローミングサーバのデジタルコンテンツ配信方法であって、前記デジタルコンテンツサーバから所定の知的財産保護システムが施されたデジタルコン

テンツを受信し、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、前記変換されたデジタルコンテンツを前記クライアントに配信することを特徴とする。

【0069】

また、上記目的を達成するために本発明の他の態様によるデジタルコンテンツ配信方法は、クライアントとネットワークを介して接続されるローミングサーバのデジタルコンテンツ配信方法であって、前記クライアントから知的財産保護システムが施されたデジタルコンテンツを受信し、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、前記変換されたデジタルコンテンツを前記クライアントに配信することを有することを特徴とする。

【0070】

【発明の実施の形態】

<実施例1>

図14は、本発明にかかわる実施例1のIPMPSystemのローミングシステムを説明する図である。

【0071】

いわゆるオフライン処理に相当し、ユーザーはコンテンツやオブジェクトデータを入手するため個々のコンテンツ・オブジェクトデータ配信サーバーへ依頼し、ユーザー認証等の正規手順後公開キー情報やパスワードパラメータ等とデータを入手した後、ユーザーAが再生に必要なIPMP System情報変換をRoaming Serviceプロバイダーへ依頼する。以下に具体的に手順を説明する。

①： ユーザーA (Type2001h IPMP System保有)がサーバーB (Type2001h IPMP System) とサーバーC (Type2021h IPMP System) からコンテンツやコンテンツのオブジェクトデータを入手し、必要な金額を支払い、ユーザー認証手続きを行って暗号解読の為のキーやパスワードパラメータ等のIPMP情報を受け取る。

②： ユーザーAの装置には再生に必要な暗号解除用Type2021h IPMP Systemが無い為、再生できない。そこでユーザーAはIPMP System Roaming ServiceプロバイダーへIPMP System情報変換を依頼する。

③：Roaming Serviceプロバイダ側で変換要求コンテンツorオブジェクトIPMP System TypeをユーザーAのIPMP System Typeへ変換できる場合、ユーザーへ必要な金額を要求し、双方の条件成立の後IPMP System情報をType2001h用へ変換し

④： ユーザーAへ返す。（通常再度この時要求したユーザーであることの認証確認が行われる。）

【0072】

### ＜実施例2＞

図15は、本発明にかかわる実施例2のIPMP Systemのローミングシステムを説明する図である。本実施例ではユーザー認証の代行サービスも行う例を示す。

【0073】

ユーザーAはIPMP System Roaming Serviceプロバイダへ入手したいコンテンツ・オブジェクトの入手を一括依頼する。Roaming Serviceプロバイダはユーザーを代行し、各コンテンツorオブジェクト配信サーバーとの認証・課金を代行し、データとキーやパスワードなどを入手した後、ユーザーAのIPMP System情報へ変換しユーザーAへ提供する。以下に具体的に手順を説明する。

①： ユーザーAはRoaming Serviceプロバイダーへ必要なコンテンツやオブジェクトの入手とユーザーAの持つType2001h IPMP SystemへのIPMP情報変換を依頼する。

②：Roaming Serviceプロバイダーはユーザーからの要求に従い、サーバーB（Type2001h IPMP System）とサーバーC（Type2021h IPMP System）へ正規手順にて必要な金額を支払ったりユーザー認証手続きを行い、コンテンツやオブジェクトデータを入手し、暗号解読の為のキーやパスワードパラメータ等を受け取る。

③： ユーザーAのType2001h IPMP Systemでの再生に必要な暗号解除が可能となるようにIPMP情報変換を行い、

④： 依頼したユーザーAとの認証を行った後、

⑤： IPMP情報変換したデータを渡す。

【0074】

図16は、図15におけるクライアント（図15のユーザーAに相当）、コンテンツサーバ（図15のサーバーB或いはサーバーCに相当）、ローミングサー

バ間でのデータ通信の工程を示した図である。

【 0 0 7 5 】

まず、クライアントがローミングサーバにコンテンツ配信要求を発する（1 6 0 1）。次に、ローミングサーバ側がユーザの認証作業を行う（1 6 0 2）。尚、ユーザ認証の方式については特に言及しない。

【 0 0 7 6 】

次に、コンテンツにかけられているセキュリティシステムのタイプをクライアントに送信する（1 6 0 3）。このとき、セキュリティのタイプは、前述したRAによってすでに登録されているものとする。

【 0 0 7 7 】

次に、クライアントにて、コンテンツサーバから送られてきたセキュリティシステムがクライアントのプレイヤのセキュリティタイプと合致するか（プレイヤでセキュリティシステムが解除可能）を検査する（1 6 0 5）。

【 0 0 7 8 】

もし、合致した場合には、クライアントからローミングサーバに対してコンテンツ配信依頼が発行される。依頼を受けたローミングサーバは、コンテンツサーバに対してこの依頼を伝達する。このとき同時に、ユーザの認証データと、ローミングサーバ自身の正当性を認証するための電子証明書が発行・伝送される（1 6 0 4）。

【 0 0 7 9 】

コンテンツサーバはローミングサーバの正当性を認証し（1 6 0 8）、もし正当だと認証された場合は、コンテンツサーバからコンテンツを配信する（1 6 1 3）。

【 0 0 8 0 】

クライアントは、セキュリティを解除し適宜圧縮されたメディアデータの復号動作などを行い（1 6 1 5）、表示・再生を行う（1 6 1 6）。

【 0 0 8 1 】

一方、セキュリティシステムタイプが合致しない場合は、クライアントからローミングサーバに対してクライアントのサポートしているセキュリティシステム

のタイプを伝送する（1606）。

【0082】

次に、ローミングサーバは、しかるべきコンテンツサーバに、ローミングサーバに対してのコンテンツの1次配信を依頼する（1607）。このとき同様に電子証明書・ユーザの認証データなどを添付する。依頼を受けたコンテンツサーバは、ローミングサーバの正当性を認証（1609）したのち、ローミングサーバにコンテンツを配信する（1610）。

【0083】

次に、ローミングサーバにおいて、コンテンツを受信し、コンテンツプロバイダから供給されたセキュリティ情報を用い、コンテンツのセキュリティを解除する。その後、セキュリティ方式の変換（トランスコンバート）を行う（1611）。

【0084】

この変換処理は、具体的には暗号などの手法によってセキュリティがかけられているコンテンツにおいて、コンテンツサーバからの情報によって暗号を解読し、クライアントが利用可能な異なった暗号方式を採用し再び暗号化したり、あるいは暗号解読後、すかし合成等を行い著作権を提示するといった方法も考えられるが、具体的な処理については特記しない。この処理後、ローミングサーバからクライアントへの送信が行われる（1612）。

【0085】

クライアントでは、ローミングサーバから送信されるコンテンツを受信後、ローミングサーバから同時に送信されるセキュリティ解除情報を使用して、コンテンツを解読する。あるいは、すかしなどが付加されている場合は、それを除去する。ビデオなどのコンテンツは通常圧縮された形で伝送されるので、適宜復号化を行い（1615）、再生・表示を行う（1616）。

【0086】

<実施例3>

図17は、本発明にかかわる実施例3のIPMP Systemのローミングシステムを説明する図である。コンテンツプロバイダからRoaming Serviceを要求する例で

ある。

①： ユーザーAはサーバーBへコンテンツやオブジェクトの入手を正規手続きで依頼する。

②： サーバーBはユーザーの持つIPMP System Typeを確認し、異なる場合にRoaming Serviceプロバイダへ正規手続きでIPMP情報交換を依頼し、必要なデータを渡す。

③： Roaming ServiceプロバイダはサーバーBからの変換要求に応じて、ユーザーAのType2001h IPMP Systemでの再生に必要な暗号解除が可能となるようにIPMP情報変換を行う。

④： IPMP情報変換したデータを渡す。

【0087】

図18は、図17におけるクライアント（図17のユーザーAに相当）、コンテンツサーバ（図17のサーバーBに相当）、ローミングサーバ間でのデータ通信の工程を示した図である。

【0088】

本例では、図16がローミングサーバに対してクライアントが要求を送信していたのに対して、コンテンツサーバに直に要求を送信したときの例である。

【0089】

まずクライアントがコンテンツサーバにコンテンツ配信要求を発する（1801）。

【0090】

次に、コンテンツサーバ側がユーザの認証作業を行う（1802）。ユーザ認証の方式については特に言及しない。

【0091】

次に、コンテンツにかけられているセキュリティシステムのタイプをクライアントに送信する（1803）。

【0092】

このとき、セキュリティのタイプは、前述したRAによってすでに登録されているものとする。次にクライアントにて、コンテンツサーバから送られてきたセキ



セキュリティシステムがクライアントのプレイヤーのセキュリティタイプと合致するか（プレイヤーでセキュリティシステムが解除可能）を検査する（1805）。

【0093】

もし、合致した場合には、コンテンツサーバからコンテンツを配信し（1804）、クライアントにてセキュリティを解除し適宜圧縮されたメディアデータの復号動作などを行い（1814）、表示・再生を行う（1815）。

【0094】

一方、セキュリティシステムタイプが合致しない場合は、コンテンツサーバに対してクライアントのサポートしているセキュリティシステムのタイプを伝送する（1806）。

【0095】

次に、コンテンツサーバは、しかるべきローミングサーバに、セキュリティの変換作業を依頼する（1807）。

【0096】

コンテンツサーバ・ローミングサーバ間では、その正当性を立証するための通信が行われる。具体的に、電子証明書を用いた方式で説明する。

【0097】

依頼を受けたローミングサーバは、その正当性を示すために、あらかじめ取得しておいた電子証明書をコンテンツサーバに対して送信する（1808）。

【0098】

上記電子証明書を受信したコンテンツサーバは、証明書を確認しローミングサーバの正当性を検証（1809）したのち、コンテンツをローミングサーバに送信する（1811）。

【0099】

次に、ローミングサーバにおいて、セキュリティ方式の変換（トランスコンバート）を行う（1812）。具体的には、暗号などの手法によってセキュリティがかけられているコンテンツにおいて、コンテンツサーバからの情報によって暗号を解読し、クライアントが利用可能な異なった暗号方式を採用し再び暗号化したり、あるいは暗号解読後、すかし合成等を行い著作権を提示するといった方法

も考えられるが、具体的な処理については特記しない。

【0100】

処理後、ローミングサーバからクライアントへの送信が行われる（1813）。クライアントでは、ローミングサーバから送信されるコンテンツを受信後、ローミングサーバから同時に送信されるセキュリティ解除情報を使用して、コンテンツを解読する。あるいは、すかしなどが付加されている場合は、それを除去する。ビデオなどのコンテンツは通常圧縮された形で伝送されるので、適宜復号化を行い、再生・表示を行う（1815）。

【0101】

<実施例4>

図19は、本発明にかかわる実施例4のIPMP Systemのローミングシステムを説明する図である。本実施例では図14、図15などの例でユーザーAとRoaming Serviceプロバイダとの間で前述の従来例で述べたOPIMA VMを持った場合の応用例である。

【0102】

本実施例では互いにOPIMA VMで構成された異なるIPMP System間で問題となった課題2、3をユーザーAの持つ一つのIPMP System Typeで済むので解消し、他の情報のやり取りなどの自動化などに有効利用できるようになる。

【0103】

図19において、51はIPMPS-Type 2000のMPEG-4コンテンツ・サーバー、52はIPMPS-Type 2001のMPEG-4コンテンツ・サーバー、53はIPMPS-Type 2002のMPEG-4コンテンツ・サーバーである。54はネットワーク、55はローミング・サーバー、56はMPEG-4プレーヤーである。

【0104】

MPEG-4プレーヤー56と、ローミング・サーバー55は、互いにOPIMAモデルのプロトコルをサポートする。

【0105】

いま、MPEG-4プレーヤー56がローミング・サーバー55に対してコンテンツの配信を要求した場合、ローミング・サーバー55は、そのコンテンツを

保有するコンテンツ・サーバー 5 1、5 2 または 5 3 にデータのダウンロードを要求する。

【 0 1 0 6 】

例えばそのコンテンツはサーバー 5 2 の中にあったとする。

【 0 1 0 7 】

この場合、ユーザー認証はローミング・サーバー 5 5 とプレーヤー 5 6 との間で成されるが、同時にコンテンツ・サーバー 5 3 とローミング・サーバー 5 5 との間でも行われても良い。

【 0 1 0 8 】

すると、コンテンツがサーバー 5 2 からネットワーク 5 4 を介してローミング・サーバー 5 5 にダウンロードされる。その手順は、上記の実施例で説明した手順でも良く、また、OPIMA方式であっても良い。ここでは、OPIMA方式でないものとする。

【 0 1 0 9 】

一方、ローミング・サーバー 5 5 とプレーヤー 5 6 との間は、OPIMA方式を採用する。MPEG-4プレーヤーが、初め、Type 2000のIPMP Systemしか持っていなかった場合、プレーヤー 5 6 は、Type 2001のIPMP Systemのダウンロードをローミング・サーバー 5 5 に要求する。ローミング・サーバー 5 5 は、殆ど全てのコンテンツ・サーバーのIPMP Systemを持っているので、それをそのまま端末 5 6 に伝送すれば良い。即ち、Type 2001のIPMP Systemをダウンロードする。

【 0 1 1 0 】

Type 2001の IPMP Systemのダウンロードが完了したら、プレーヤー 5 6 はIPMP Systemを Type 2000からType 2002に切り替え、互換性のあるS-Typeでエンドツーエンドの通信ができる。

【 0 1 1 1 】

実施例 4 により、データ配信に遅延が発生せず、リアルタイム性を維持できる。

【 0 1 1 2 】

<上記実施例のサービスを実現する具体的Service Request仕様例>

図 2 0 では本件のサービスを実行する場合のユーザーやコンテンツプロバイダが IPMP 情報交換サービス要求する際の基本的共通情報を例示している。

【 0 1 1 3 】

コンテンツ or オブジェクトが MPEG-4 IPMP 情報を持つ場合には図 1 2 で示したように、図 2 0 に図示した国際標準仕様に記載された「IPMP Message」データ構造を持っている。このデータの先頭に Registration Authority 登録された unique な IPMP System ID が含まれるので、ユーザー A が入手した、或いはしようとするコンテンツ or オブジェクトデータのセキュリティが Type 何番の IPMP System かを知ることが出来る。

【 0 1 1 4 】

一方、Roaming Service プロバイダーは

- 1) 変換要求したユーザー A の持つ IPMP System Type を知る必要があること、
  - 2) 変換後のデータを返す為にユーザー A の持つ再生装置を特定する必要があること、
  - 3) 変換を要求されたデータ自身か又はデータの入手先情報、
- の 3 点は最低限必要となる。

【 0 1 1 5 】

このような Roaming Service に必要な事項は IPMP System Type によらず共通しており、ユーザー A や Roaming Service プロバイダーに共通した情報である。

【 0 1 1 6 】

そこでサービス要求時に Roaming Service プロバイダーが異なってもサービスが受けられる為に、図 2 0 で図示・提案されている data 構造を back channel 経由で交換できれば、よりスムーズな Roaming Service が世界標準的規模で得られることが可能となる。

【 0 1 1 7 】

Roaming Service Request を図 2 0 の提案する (Roaming Service Syntax) データ構造で伝える手段として、より標準的手法は通常使用では downstream 処理の (MPEG-4 bitstream を受け取りシーン再生処理する) Player 側から図 2 0 に示される Upchannel information として Roaming Service Request 情報を Upstream 処理

(いわゆるMPEG-4でのback channel機能を使い、player側からサーバー側へ情報を配信する機能) するためにプレイヤからストリームを返すためのフラグ仕様があり本実施例ではこの機能を使って例示している。

## 【0118】

ここで、本発明にかかわるback channel実施の形態を図面を参照しながら説明する。

## 【0119】

図21は、本発明の好適な実施の形態に係るMPEG-4プレーヤーを含むシステムの概略構成を示す図である。図4に示すシステムは、「IP Data Set」を操作して「IP Protection」を実現するシステムである。図4に示すシステムは、IPMPS (Intellectual Property Management and Protection System) 207を有し、このIPMPS 207により著作権認証及び保護機能を実現する点で図3に示すシステムと異なる。

## 【0120】

図22は、認証処理に関するクライアントの動作を示すフローチャートである。以下、図22を参照しながら図4に示すシステムの動作を説明する。サーバー側では、マルチプレクサ201が、各々異なるURL (Uniform Resource Locator) としてURL1、URL2、URL3を持つ複数のネットワーク・サイト201~204から、夫々個々のオブジェクトを受信してこれらの複数のオブジェクトで構成される動画データを生成する。この動画データは、クライアントからの要求に応じてMPEG-4ビットストリーム205としてネットワークを介してクライアントに送信される。

## 【0121】

ステップS1では、クライアントは、サーバーよりMPEG-4ビットストリーム205を受信する。このMPEG-4ビットストリームを構成する各オブジェクトには、著作権の帰属先を示す情報(ここでは、URLの情報)が付随している。ステップS2では、クライアントは、受信に係るMPEG-4ビットストリームをデマルチプレクサ206により複数のオブジェクトやそれに付随する情報(URLの情報を含む)等の複数のストリームに分離する。ここで、各オブジ

ェクトに付随するURLの情報は、「IP Data」のストリームである「IPMP Stream」の一部としてIPMPS 2 0 7に送られる。

【0 1 2 2】

ステップS 3では、IPMPS 2 0 7に送られた1又は複数のURLの情報の中から、いずれか1つのURLの情報を選択する。これは、例えば、操作者が指定するものであっても構わないし、所定の順序に従ってIPMPS 2 0 7が選択しても構わない。

【0 1 2 3】

ステップS 4では、選択したURLの情報に基づいて、ネットワーク上に接続された1又は複数のサーバのうち対応するURLを持つサーバ2 0 1に対して認証依頼信号を送信する。この場合、その送信には、後述するバックチャネル (back-channel) 1又はバックチャネル (back-channel) 2が使用される。

【0 1 2 4】

ステップS 5では、認証依頼信号を受け取ったサーバ2 0 1からアクセス許可信号が送信されてくるのを待ち、アクセス許可信号を受信した場合はステップS 6に進み、所定時間内にアクセス許可信号を受信しなかった場合はステップS 7に進む。

【0 1 2 5】

ステップS 6では、アクセス許可信号の受信によりアクセス許可（認証）が得られたオブジェクトに対するアクセスを可能にする。具体的には、アクセスコントロールポイントを制御する制御信号2 1 2を許可状態にすることにより、シーン・ディスクリプタ2 0 8、オーディオ・ビジュアル・デコーダ2 0 9、オブジェクトディスクリプタ2 1 0がデマルチプレクサ2 0 6の該当するストリーム（即ち、アクセス許可信号によりアクセスを許可されたオブジェクトのストリーム）にアクセスすることを可能にする。

【0 1 2 6】

一方、ステップS 7では、アクセスコントロールポイントを制御する制御信号2 1 2を禁止状態にすることにより、シーン・ディスクリプタ2 0 8、オーディオ・ビジュアル・デコーダ2 0 9、オブジェクトディスクリプタ2 1 0がデマル

チプレクサ 2 0 6 の該当するストリーム（即ち、認証を依頼したがアクセス許可が得られなかったオブジェクトのストリーム）にアクセスすることを禁止する。

【 0 1 2 7 】

ステップ S 8 では、他のオブジェクトに付随する URL の情報があるか否かを確認し、当該 URL の情報があればステップ S 3 に戻り、なければ一連の処理を終了する。

【 0 1 2 8 】

シーン合成・グラフィック処理部 2 1 1 は、シーン・ディスクリプタ 2 0 8、オーディオ・ビジュアル・デコーダ 2 0 9、オブジェクトディスクリプタ 2 1 0 から供給されるデータに基づいて、シーン合成及びグラフィック処理を行う。この際、アクセス許可が得られたオブジェクトのみを再生の際の合成の対象としても良いし、1 つでもアクセス許可が得られなかったオブジェクトがある場合に、一切の再生を行わないようにしても良い。

【 0 1 2 9 】

以下、上述した認証処理について更に詳細に説明する。

【 0 1 3 0 】

MPEG-4 ビットストリームは、オブジェクト単位のビットストリームである「Elementary Stream」(ES) の内容を記述する「ES\_Descriptor」と、オブジェクト自身を記述する「OD\_Descriptor」を含む。ここで、「ES\_Descriptor」或いは「OD\_Descriptor」に、リモートアクセスのためのコマンドとアクセス先を指定する URL の情報が含まれている場合は、図 5 に示すような手順でリモートアクセスが実行される。

【 0 1 3 1 】

図 2 3 は、リモートアクセスを説明する簡略図である。

【 0 1 3 2 】

図 2 3 において、「DAI」は、「DMIF Application Interface」と呼ばれる、MPEG-4 ビットストリームとネットワークとのインターフェース層である。この詳細については、「ISO/IEC 14496-6 DMIF ドキュメント DMIF Application Interface」の項に記載されているため、ここでは省略する。

## 【 0 1 3 3 】

また、MPEG-4 ビットストリームは、「elementary stream」 (ES) に対応したデコーダの種類についての情報を示す「DecoderConfigDescriptor」を含む。この「DecoderConfigDescriptor」は、幾つかのデータ要素の構造体であり、その中の要素の一つにストリーム型を示す1ビットのupStreamパラメータがある。この詳細については、「ISO/IEC 14496-1 FCD 8.3.4DecoderConfigDescriptor」の項に記載されているため、ここでは省略する。

## 【 0 1 3 4 】

式1に、「DecoderConfigDescriptor」の一例を挙げる。

[式1 : DecoderConfigDescriptor]

```
aligned(8) class DecoderConfigDescriptor
{
    : bit(8) tag=DecoderConfigDescrTag {
    bit(8) length;
    bit(8) objectProfileIndication;
    bit(6) streamType;
    bit(1) upStream;
    const bit(1) reserved=1;
    bit(24) bufferSizeDB;
    bit(32) maxBitrate;
    bit(32) avgBitrate;
    DecoderSpecificInfo decSpecificInfo[];
}
```

## 【 0 1 3 5 】

ここで、ストリームの識別は、式1の「DecoderConfigDescriptor」のクラス宣言中のデータ要素である「streamType」の値に基づいて行う。「streamType」の値は、表3のように定義されている。

## 【 0 1 3 6 】



【表 3】

表 3：ストリーム型指定値

ストリーム型指定値	ストリーム型
0x00	reserved for ISO use
0x01	ObjectDescriptorStream
0x02	ClockReferemceStream
0x03	SceneDescriptionStream
0x04	VisualStream
0x05	AudioStream
0x06	MPEG7Stream
0x07	IPMPSteam
0x08, 0x09	reserved for ISO use
0x0A	ObjectContentInfoStream
0x0C-0x1F	reserved for ISO use
0x20-0x3F	user private

## 【0 1 3 7】

なお、表 3 は、「ISO/IEC 14496-1 FCD Table 0-1: streamType Values」に対して、この実施の形態に固有の「IPMPStream」を識別するための値を追加したものである。表 3 において、各パラメータや用語は、「ISO/IEC 14496-1 FCD」と同じであるので、ここでは説明を省略する。

## 【0 1 3 8】

図 2 1 に示すように、ストリームの向きを示すフラグである「DecoderConfigDescriptor. upStream」が ” 1 ” の時は、システムは、クライアント側からサーバ側にストリームを転送する「upstream」の状態になる。ここでは、この「upstream」の状態を利用した転送機能を「back-channel 1」と呼ぶことにする。

## 【0 1 3 9】

通常の再生時は、「DecorderConfigDescriptor. upStream」が ” 0 ” であり、サーバ側からクライアント側にストリームを転送する「downstream」の状態である。一方、オブジェクトに対するアクセスの許可を求める場合は、「DecorderCo

「nfigDescriptor. upStream」を” 1 ”として、必要なデータをURL先へ「upstream」する所謂「back-channel 1」を用いることにより、「IPMP Management Data」（著作権管理情報）を「IPMPStream」としてサーバ側に送り、リモートアクセスによりURL先から応答データを転送させることになる。

【 0 1 4 0 】

表3に示す「IPMPStream」は、「IPMP\_ES」と「IPMP\_D」の構成を有する。「IPMP\_ES」の各々は一連の「IPMP\_Messages」からなる。

【 0 1 4 1 】

式2は「IPMP\_Messages」の記述例である。

【 0 1 4 2 】

[式2:IPMP\_Message]

```
class IPMP_Message () {
    unsigned int(8)    IPMPS_TypeCount;
    bit(1)  hasURL;
    int i;
    for (i = 0; i < IPMPS_TypeCount; i++) {
        unsigned int(16) IPMPS_Type[[i]];
        unsigned int(32) offset[[i]];
        unsigned int(16) length[[i]];
    }
    if (hasURL) {
        unsigned int(5) lengthOfURLbits;
        bit(3) reserved=0b111;
        unsigned int(lengthOfURLbits) lengthOfURL;
        char(8) URLString[lengthOfURL];
    }
    for (i = 0; i < IPMPS_TypeCount; i++) {
        char(8) IPMP_data[length[i]];
    }
}
```

}

## 【 0 1 4 3 】

式 2 において、「IPMPS\_TypeCount」は、異なる「IPMPS type」の数を表わす。これにより、異なる IPMPS を存在させることが可能となるため、「IPMP messages」は複数の IPMPS に対応可能である。

## 【 0 1 4 4 】

なお、URL が指定されている場合は、「IPMPS\_TypeCount」は 0 を取り、その他は最低値である 1 を取る。また、この場合、内部の「IPMP\_Message」の代わりに、外部に格納されている「IPMP\_Message」を参照して使用することになる。

## 【 0 1 4 5 】

また、「IPMPS\_D」は、「IPMP Descriptor」からなる。この「IPMP Descriptor」は、個々の「elementary streams」に対する詳細な IPMP 制御を行うためのデータ構造体である。そして、「IPMP Descriptor Updates」は、オブジェクト・ディスクリプタ・ストリーム (Object Descriptor stream) の一部として実行される。式 3 は、「IPMP Descriptor Updates」の記述例を示す。

## 【 0 1 4 6 】

[式 3: IPMP\_DescriptorUpdate]

```
aligned(8) class IPMP_DescriptorUpdate : uint(8) IPMP_DescriptorUpdateTag {
    unsigned int(8)    descriptorCount;
    int i;
    for (i = 0; i < descriptorCount; i++) {
        IPMP_Descriptor    d[[i]];
    }
}
```

## 【 0 1 4 7 】

式 3 において、「descriptorCount」は、更新される「IPMP\_Descriptors」の数を表わし、また、d [ i ] は、ある一つの「IPMP\_Descriptor」を表わす。

## 【 0 1 4 8 】

式 4 は、「IPMP\_Descriptor」の記述例を示す。

【 0 1 4 9 】

[式4:IPMP\_Descriptor]

```
class IPMP_Descriptor () {
    bit(8)  IPMP_Descriptor_ID;
    unsigned int(8)    IPMPS_TypeCount;
    bit(1)  hasURL;
    int i;
    for (i = 0; i < IPMPS_TypeCount; i++) {
        unsigned int(16)    IPMPS_Type[[i]];
        unsigned int(32) offset[[i]];
        unsigned int(16) length[[i]];
    }
    if (hasURL) {
        unsigned int(5) lengthOfURLbits;
        bit(3) reserved=0b111;
        unsigned int(lengthOfURLbits) lengthOfURL;
        char(8)  URLString[lengthOfURL];
    }
    for (i = 0; i < IPMPS_TypeCount; i++) {
        char(8) IPMP_data[length[i]];
    }
}
```

【 0 1 5 0 】

式 4 において、「IPMP\_Descriptor\_ID」は、各「IPMP\_Descriptor」に固有の番号であり、「ES\_Descriptors」は、「IPMP\_Descriptor\_ID」を使って「IPMP\_Descriptors」を参照する。また、「IPMPS\_TypeCount」は、「IPMP\_Message」で指定された異なる I P M P S の数を表わす。

【 0 1 5 1 】

図 2 4 は、URL 先で更に URL 指定がある場合の階層構造の例を示す図である。なお、図 2 4 に 2 階層の場合の例であるが、もちろん、更なる URL 指定がある場合、3 階層になっても 4 階層になってもよい。また、図 2 4 においては、「IPMPStream」を明示していないが、リモート指定されるオブジェクト (Object) に関する「IPMP\_ES」か「IPMP\_D」が、「SceneDescriptionStream」か「ObjectDescriptionStream」に呼応して、必要に応じデコードされ、リモートアクセスされることは、先に説明した図 2 3 の場合と同様である。

## 【 0 1 5 2 】

以上、MPEG-4 のビットストリームの「upstream」の状態、即ち、バックチャネル (back-channel) 1 を使用した認証処理について説明したが、このような「back-channel 1」を使用する認証処理は、リアルタイムのビットストリーム再生時における「upStream」処理であるので、比較的データ量が少なく処理時間の短い高速処理向けの場合を想定している。ここで、リアルタイム再生をしているシステムでは、「back-channel 1」によるリモートアクセス及び認証による遅延は極力少ないことが望ましい。

## 【 0 1 5 3 】

しかしながら、データ量が少ない場合であっても認証に相応の時間を要することがあり、その場合、「back-channel 1」における遅延が問題となる。この場合、許容遅延時間の点、また、インタラクティブな操作性を必要とする点から考えると、第 2 の「back-channel」を設けることが好ましい。

## 【 0 1 5 4 】

そこで、この実施の形態では、MPEG-4 のビットストリームを伝送するのとは異なる I/O (機器間入出力) インターフェースが設けられている。これを以下では「back-channel 2」と呼ぶことにする。

## 【 0 1 5 5 】

まず、「back-channel 2」を使用した認証処理を説明する前に、「back-channel 1」と「back-channel 2」におけるデータ量と遅延時間の関係を考える。「MPEG-4 Requirement Group」の報告では、リアルタイム再生を妨げない「back-channel」の遅延許容時間は 1 フレーム時間とあるので、これに基づいて「back-chann

el 1」と「back-channel 2」における想定データ量と転送レートの関係を求めると、表4のようになる。

【0156】

【表4】

表記	使用目的	データ量	遅延時間
back-channel 1	認証のための高速IPMP リモートアクセス	3000-5000 bits/s	100-300 ms
back-channel 2	認証のための低速IPMP 入出力アクセス		>500 ms

【0157】

ここで、認証のための高速IPMPリモートアクセスでは、100-500 bit/Frame以内のデータ量を3K-5K/secの転送ラインで処理することが遅延時間の限界となる。「IPMP\_Message」データや「IPMP\_Descriptor」データとURL指定による「back-channel」による「remote content access」の結果としてのdelay-bandwidthの関係を、表5と見ることができるので、実際の認証のためのデータ量は限られたものになる。一方、認証には、stream処理とは非同期に時間を要することが多い。

【0158】

また、複数のオブジェクトの認証が一箇所のサイトではなく、複数に跨ることも想定される。この場合には、表4の条件は更に厳しくなり、実用に耐えなくなる。そのため、stream処理と非同期で低速処理が可能な認証手続きの場合には、「back-channel 2」を用いた方が良い。

【0159】

以下、「back-channel 2」を使用した場合の処理について説明する。認証のための低速IPMP入出力アクセスのための「back-channel 2」は、図21に示すように、基本的にはMPEG-4ビットストリームを伝送するものとは異なるI/O（機器間入出力）インターフェースを対象としたものになる。

【0160】

ここで、「back-channel 2」の先に、キーボードとディスプレイとモデムを有するコンピュータ端末 2 1 4 を用意し、電話回線と I P M P S 2 0 7 とに接続する。この構成において、コンピュータ端末 2 1 4 は、認証の必要なストリーム中のオブジェクトとその認証先の情報を I P M P S 2 0 7 から受け取り、その情報をディスプレイに表示する。操作者は、その表示を参照して、認証の必要なストリーム中のオブジェクトを選択する。コンピュータ端末 2 1 4 は、認証先に電話をかけて、認証方法やアクセスコードを該認証先から受け取り、その内容をディスプレイに表示する。操作者が、受け取った情報をキーボードを使って入力すると、その入力情報が I P M P S 2 0 7 に通知され、必要なオブジェクトに対するアクセスを許可状態にする。

## 【 0 1 6 1 】

ここでは、電話回線を利用する場合を例として挙げたが、この代わりに、例えば、CATVのケーブルや無線通信路を利用しても良い。

## 【 0 1 6 2 】

また、場合によっては、予め認証先との契約において入手したアクセス認証に必要な情報を格納した P C C a r d をコンピュータ端末 2 1 4 内の P C M C I A インターフェースに差し込んで、アクセス認証に必要な情報を I P M P S 2 0 7 に通知して、オブジェクトに対するアクセスを許可状態にしてもよい。

## 【 0 1 6 3 】

なお、操作時間や認証時間がある程度長くなる認証処理の場合は、ストリーム再生の開始時やシーンチェンジ時等、リアルタイムでない場合に有効である。

## 【 0 1 6 4 】

このように、この実施の形態によれば、用途に応じて「back-channel 1」又は「back-channel 2」を選択して使用することができる。この選択は、操作者が行うことができるように構成してもよいし、システム内部で遅延時間限界等を考慮して最適な方を選択するようにしてもよい。

## 【 0 1 6 5 】

以上のように、2種類の異なる「back-channel」を設けることにより、柔軟性の高い認証処理を実現することができる。

【 0 1 6 6 】

なお、本発明は、複数の機器から構成されるシステムに適用しても、一つの機器からなる装置に適用してもよい。

【 0 1 6 7 】

また、上記の実施の形態に係る装置又は方法を構成する構成要素の全体のうち一部の構成要素で構成される装置又は方法も、本件出願に係る発明者が意図した発明である。

【 0 1 6 8 】

また、上記の実施の形態に係る装置の機能は、プログラムコードを記録した記憶媒体をシステム或いは装置に固定的又は一時的に組み込み、そのシステム或いは装置のコンピュータ（又はCPU若しくはMPU）が該記憶媒体に格納されたプログラムコードを読み出して実行することによっても達成される。ここで、該記憶媒体から読み出されたプログラムコード自体或いは該記憶媒体自体が法上の発明を構成する。

【 0 1 6 9 】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、ROM等が好適であるが、他のデバイスを採用することもできる。

【 0 1 7 0 】

また、コンピュータが記憶媒体から読み出したプログラムコードを実行することにより本発明の特有の機能が実現される場合のみならず、そのプログラムコードによる指示に基づいて、コンピュータ上で稼働しているOS（オペレーティングシステム）等が実際の処理の一部又は全部を負担する実施の態様も本発明の技術的範囲に属する。

【 0 1 7 1 】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備えられたメモリに書込まれた後に、そのプログラムコードの指示に基づいて、その機能



拡張ボードや機能拡張ユニットに備えられたCPU等が実際の処理の一部又は全部を負担する実施の態様も本発明の技術的範囲に属する。

【0172】

以上説明したように、本実施例ではクライアント・ユーザーとコンテンツ提供サーバー側との間において、入手しようとするコンテンツやオブジェクトデータがセキュリティのための暗号化や電子透かし化とそれらを解除する為に必要な公開キーやパスワード等のprivate IPMP dataが図12に図示された相互互換性のある国際標準仕様で構成されたMPEG-4データに付与されている場合を例として、以下のセキュリティで保護されたデジタルコンテンツデータの配信サービスを提供することができる。

【0173】

1. ユーザーの再生しようとするコンテンツやオブジェクトのIPMP情報を、ユーザーの持つ再生装置が有するIPMP System情報へ変換するサービスを行う。この場合の入手コンテンツやオブジェクトデータは変換後、国際標準仕様から構成された相互互換性のあるMPEG-4データ部分は変更されず、そのデータへのセキュリティのための暗号化や電子透かし化とその解除に必要な公開キーやパスワードなどのprivate IPMP dataが対象ユーザのIPMP System用に変換されるため、コンテンツやオブジェクトデータのセキュリティは保たれている。

【0174】

2. 1つのコンテンツが複数の異なるIPMP情報を持つオブジェクトからなる場合の各IPMP Systemサーバー側とのユーザー認証をユーザーからの要求等によって代行するサービスを行う。

【0175】

上述の課題で見たように、IPMP共通プラットフォームを持つことも、一つの標準IPMP Systemを定めることもそれぞれ問題を持つ。

【0176】

そこで、上記1.、2.のサービスをもつ中間的デジタルコンテンツ配信サービスプロバイダーの存在によって、結果として

1) ユーザーは再生しようとする装置のIPMP Systemと異なるIPMP System情報

を持ったコンテンツや複数のオブジェクトからなるコンテンツの再生が可能となり、

2) 一方、元々のコンテンツ・オブジェクトデータ配信側ではセキュリティを一般ユーザーへ開示する必要も無く、

3) かつ、1つの標準的なIPMP System仕様へ統一する必要も無いため、

4) content(or object) right holderの要求に応じたセキュリティシステムが構築でき、

5) ユーザーからみた操作性や異なるIPMP Systemからの制約が解消し、

6) コンテンツ・オブジェクトデータ供給側IPMP Systemのユーザーに対する interoperabilityが得られる、  
ことになる。

【0 1 7 7】

【発明の効果】

以上説明したように本発明によれば、ユーザーは再生しようとする装置の知的財産保護システムと異なる保護システムを持ったコンテンツや複数のオブジェクトからなるコンテンツの再生が可能となり、一方、元々のコンテンツ・オブジェクトデータ配信側ではセキュリティを一般ユーザーへ開示する必要も無く、かつ、1つの標準的な知的財産保護システム（例えば、IPMP System）仕様へ統一する必要も無いため、content(or object) right holderの要求に応じたセキュリティシステムが構築でき、ユーザーからみた操作性や異なる知的財産保護システムからの制約が解消し、コンテンツ・オブジェクトデータ供給側知的財産保護システムのユーザーに対する interoperabilityが得られるという優れた効果を有する。

【図面の簡単な説明】

【図 1】

従来のデジタル映像データの送受信システムを示す図である。

【図 2】

従来のMPEG-4 プレーヤーの構成図である。

【図 3】

図 2 を模式化・簡略化した図である。

【図 4】

図 3 に IPMP System 処理部を追加した図である。

【図 5】

MPEG-4 プレーヤーの内部機能ブロックダイアグラムとデータの流れを示している。

【図 6】

図 5 のデータ処理プロセスを簡略化して示した図である。

【図 7】

MPEG-4 オブジェクトアクセスデータユニットの時間調整のデータ処理例を示すフローチャートである。。

【図 8】

Decoding Buffer と Composition Memory のデータ移動とタイミングを示す図である。

【図 9】

図 6 に IPMP System 処理部を加えた場合のデータ処理プロセスを示す図である。

【図 10】

図 4 の IPMP System の動作例を示すフローチャートである。

【図 11】

IPMPDescriptor と IPMPMessage を説明するための図である。

【図 12】

ユーザーが外部サーバーから MPEG-4 コンテンツを入手し再生する例を示す図である。

【図 13】

ユーザーが外部サーバーから MPEG-4 コンテンツを入手し再生する他の例を示す図である。

【図 14】

本発明にかかわる実施例 1 の IPMP System のローミングシステムを説明する図

である。

【図 1 5】

本発明にかかわる実施例 2 の IPMP System のローミングシステムを説明する図である。

【図 1 6】

図 1 5 における処理過程を説明する図である。

【図 1 7】

本発明にかかわる実施例 3 の IPMP System のローミングシステムを説明する図である。

【図 1 8】

図 1 7 における処理過程を説明する図である。

【図 1 9】

本発明にかかわる実施例 4 の IPMP System のローミングシステムを説明する図である。

【図 2 0】

本発明にかかわり実施例のローミングサービスを実現するための具体的な Service Request の仕様を説明する図である。

【図 2 1】

本発明の好適な実施の形態に係る back channel を行う MPEG-4 プレーヤーの構成図である。

【図 2 2】

認証処理に関するクライアントの動作を示すフローチャートである。

【図 2 3】

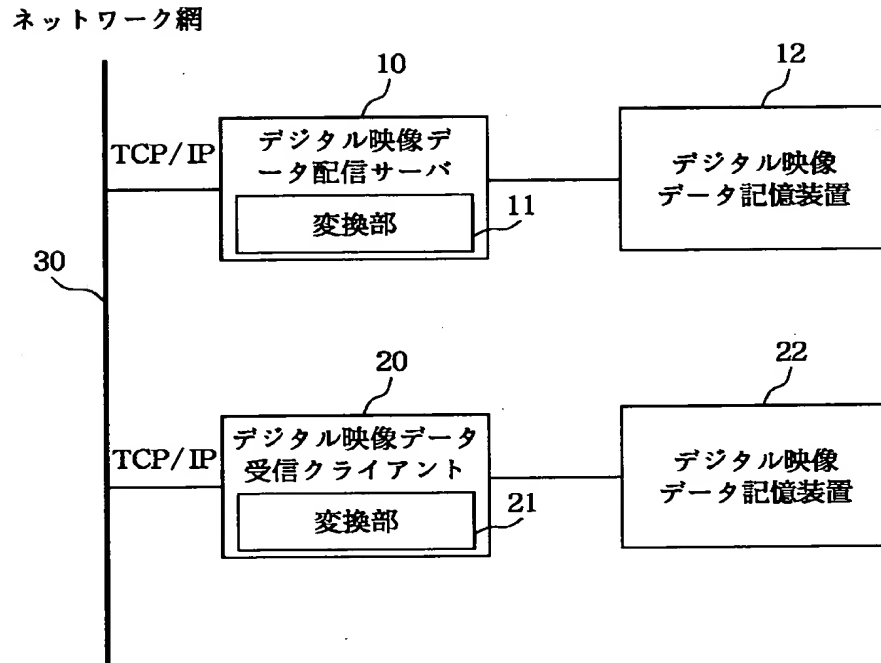
リモートアクセスを説明するための簡略図である。

【図 2 4】

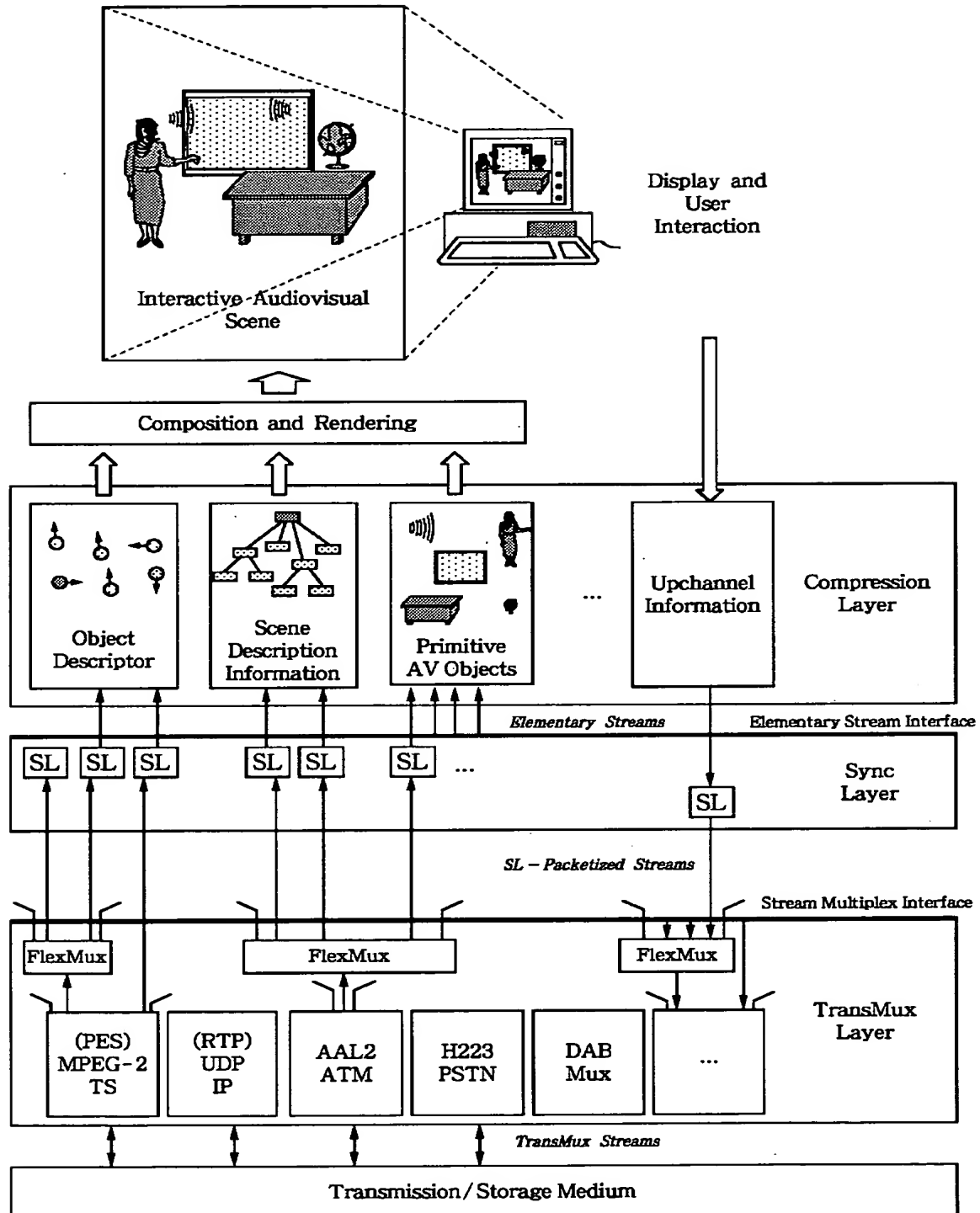
URL 先で更に URL 指定がある場合の階層構造の例を示す図である。

【書類名】 図面

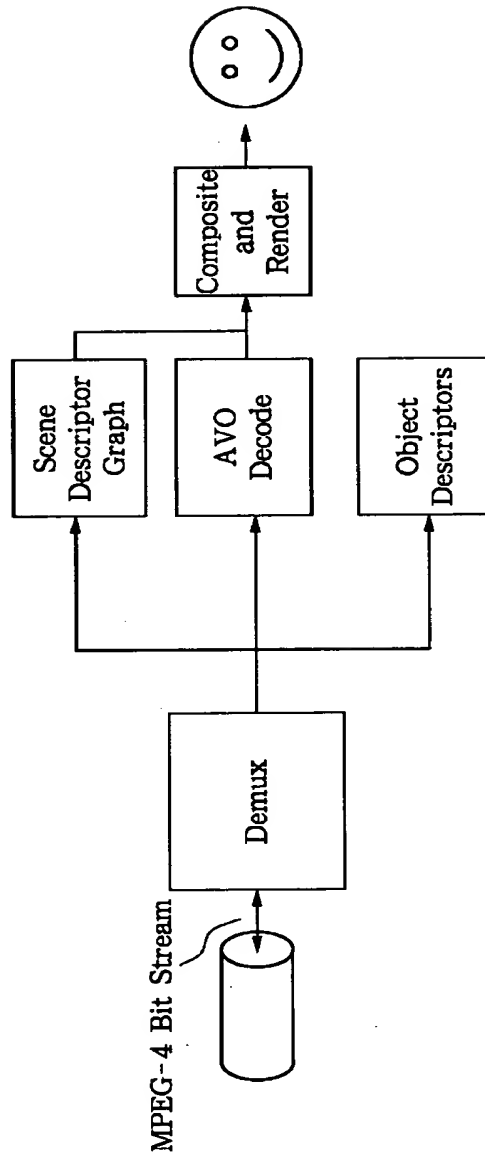
【図1】



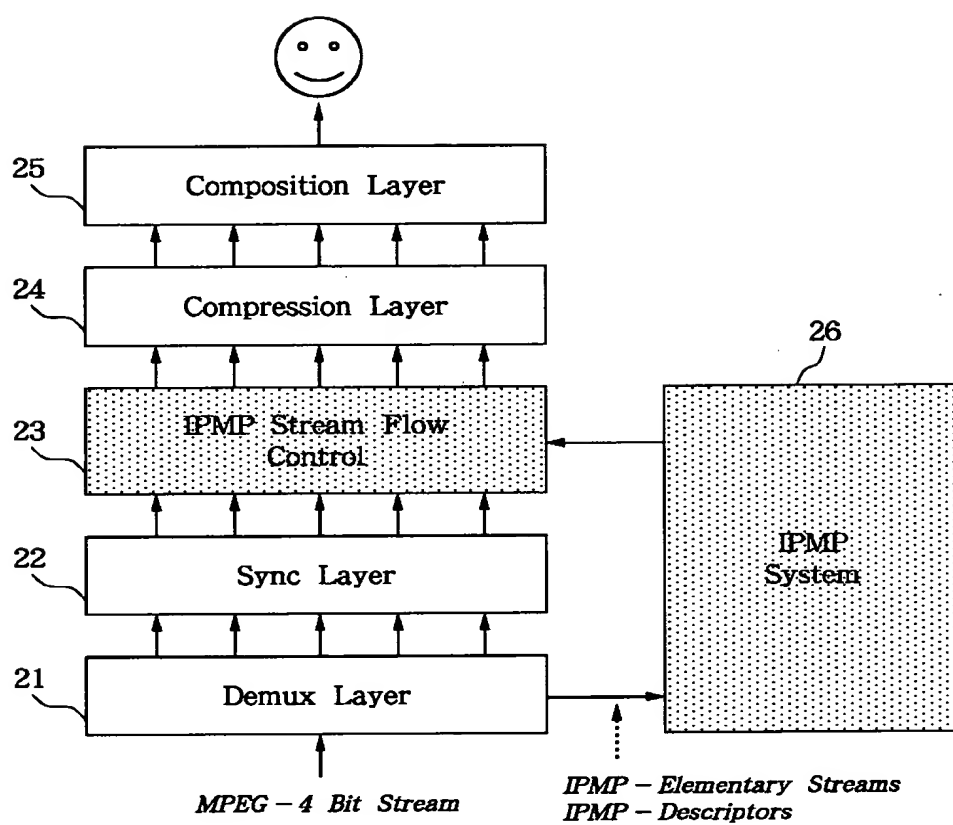
【図 2】



【図 3】

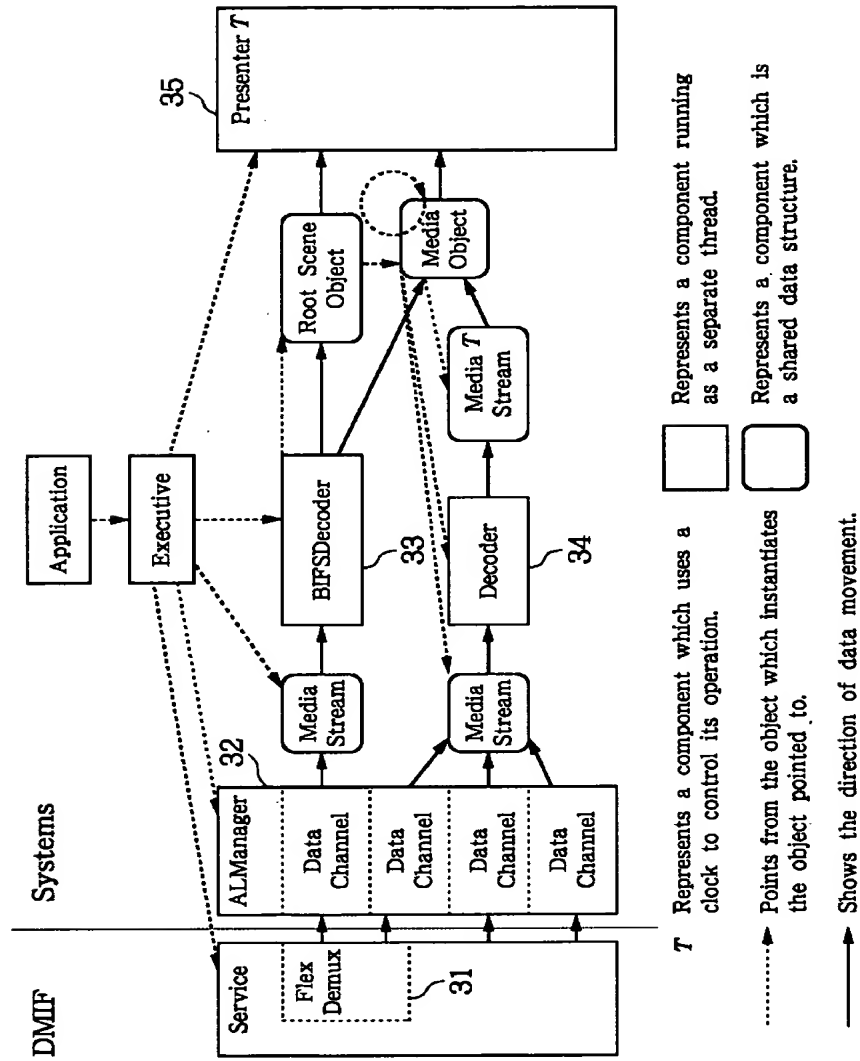


【図 4】

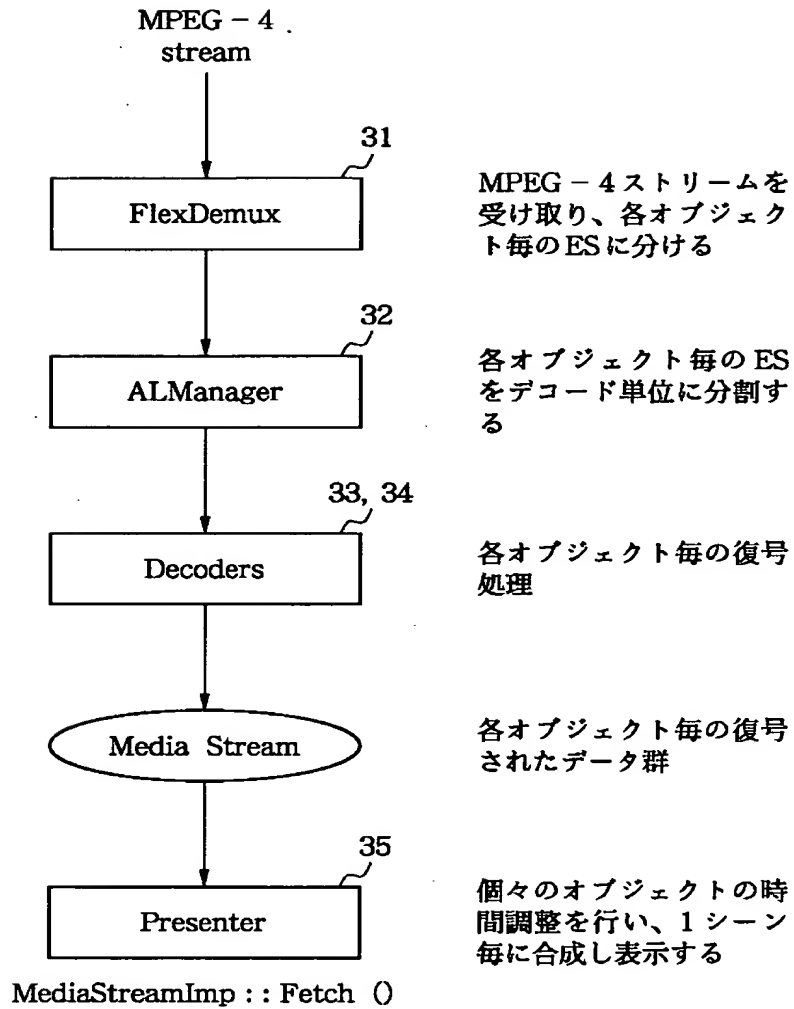




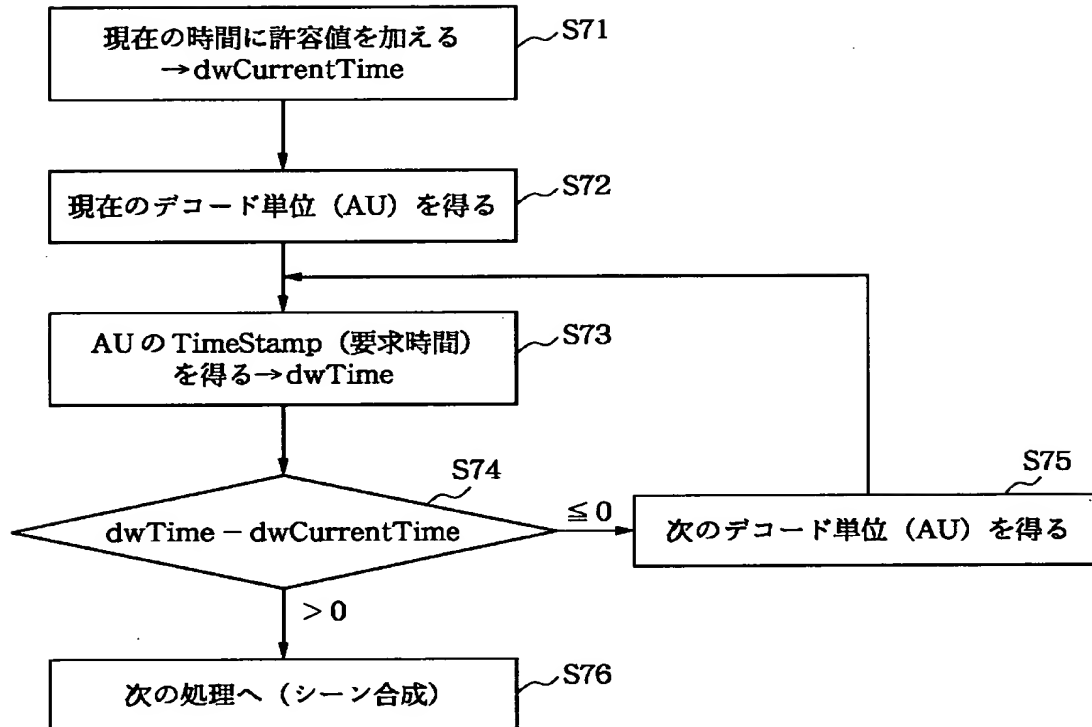
【図 5】



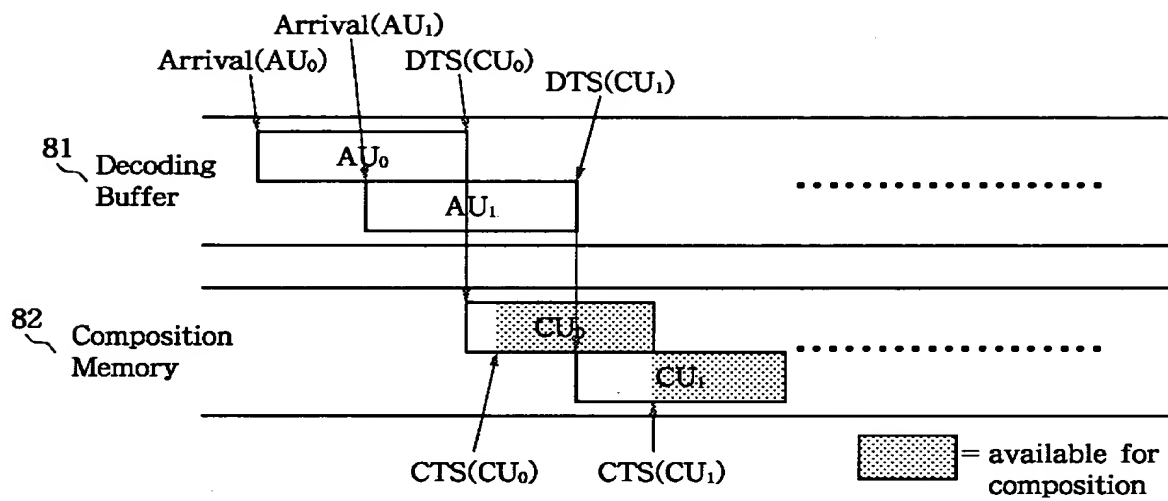
【図 6】



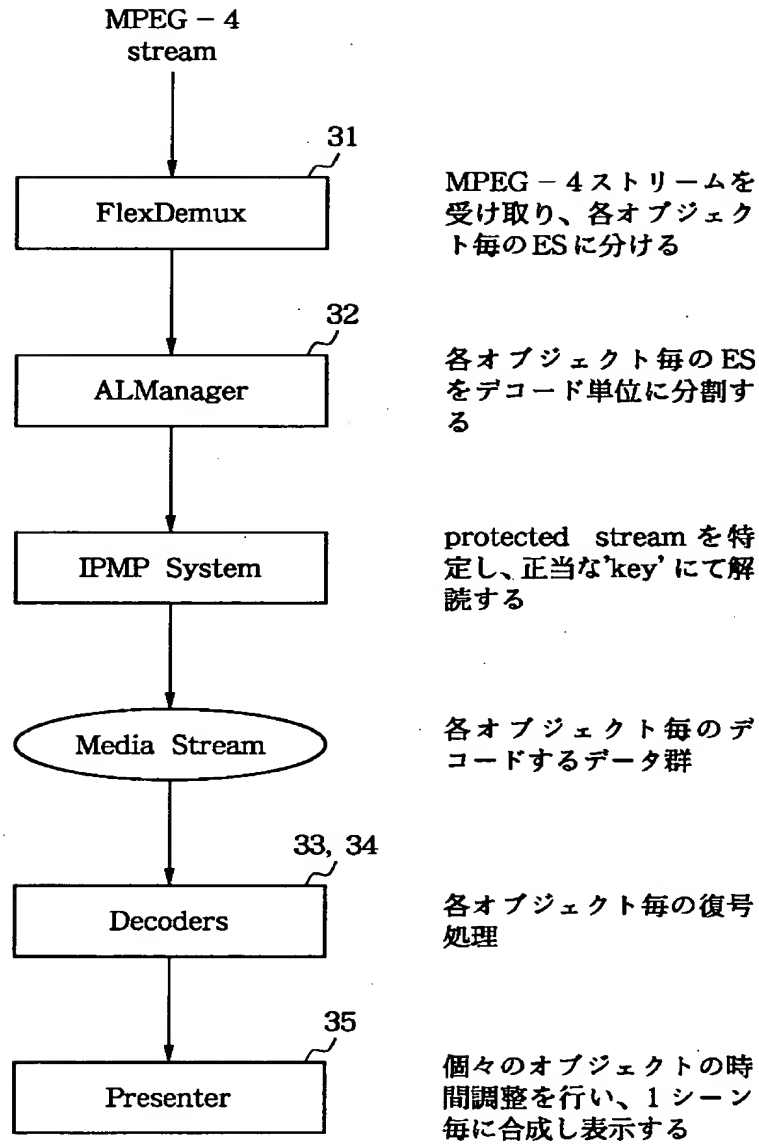
【図 7】



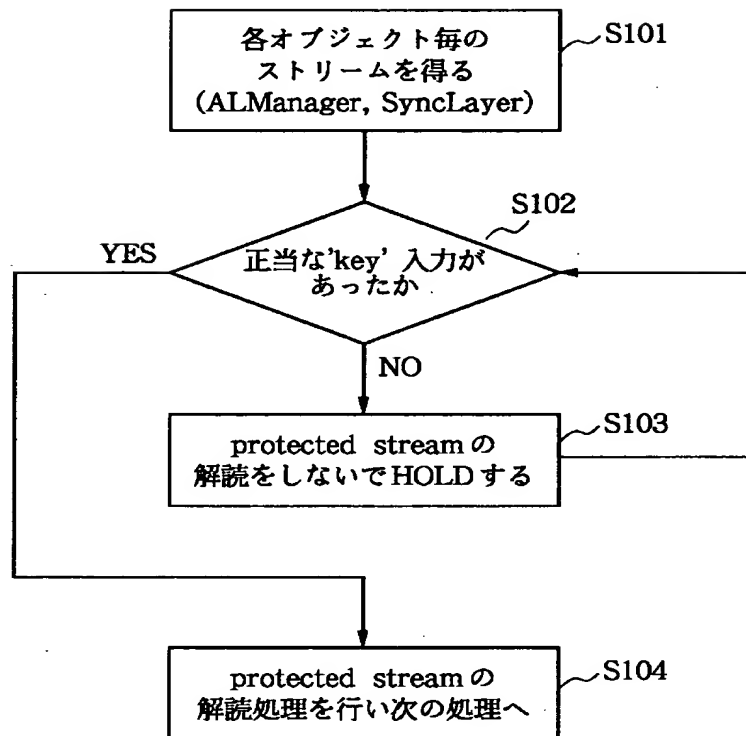
【図 8】



【図 9】

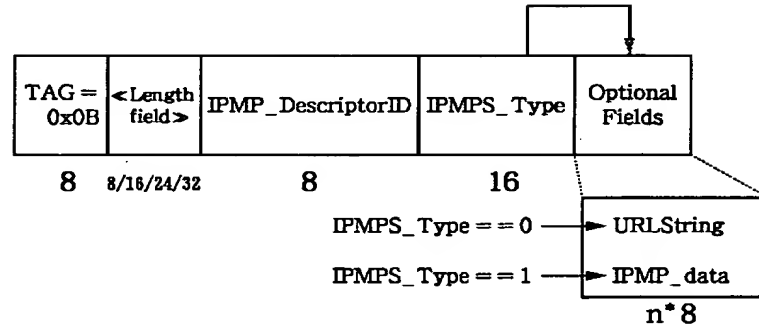


【図 1 0】

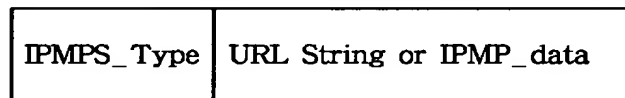


【図 1 1】

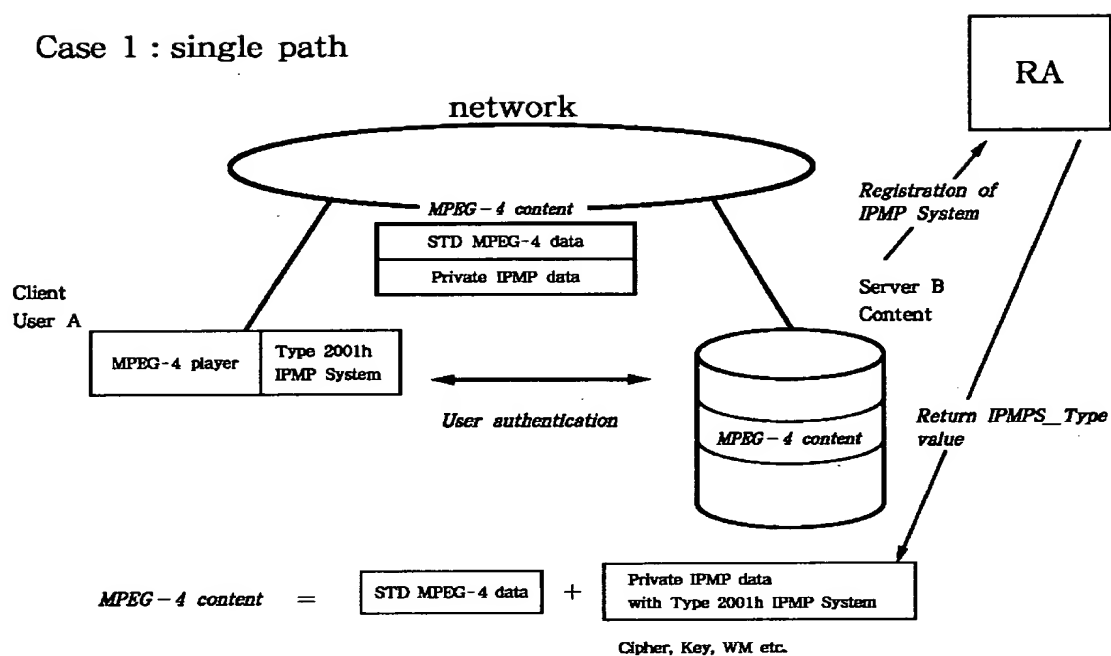
IPMPDescriptor



IPMPMessage



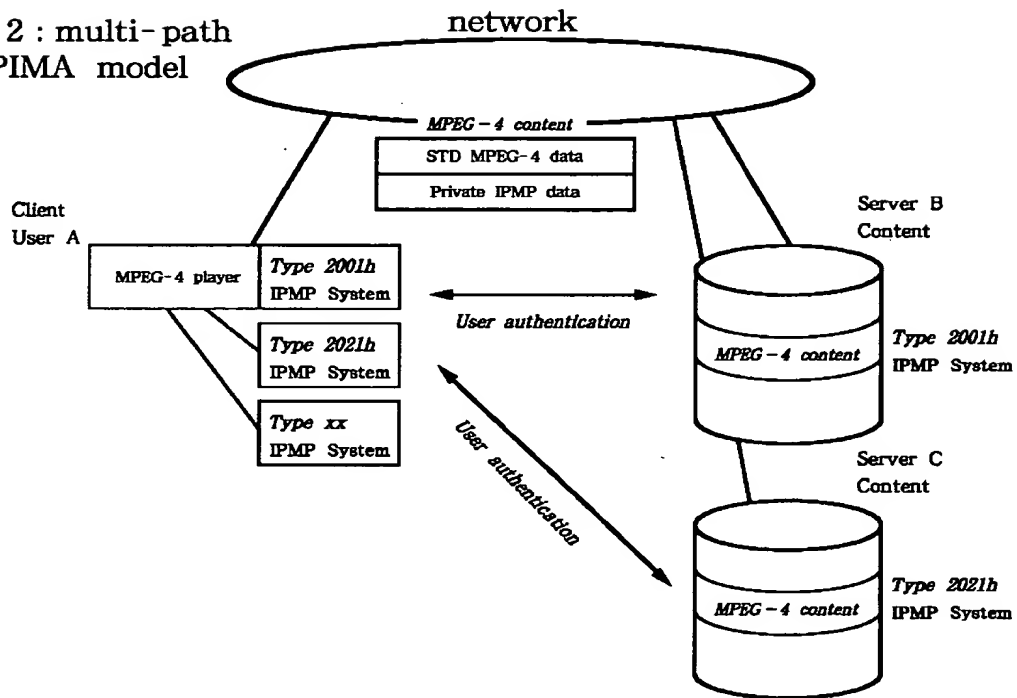
【図 1 2】



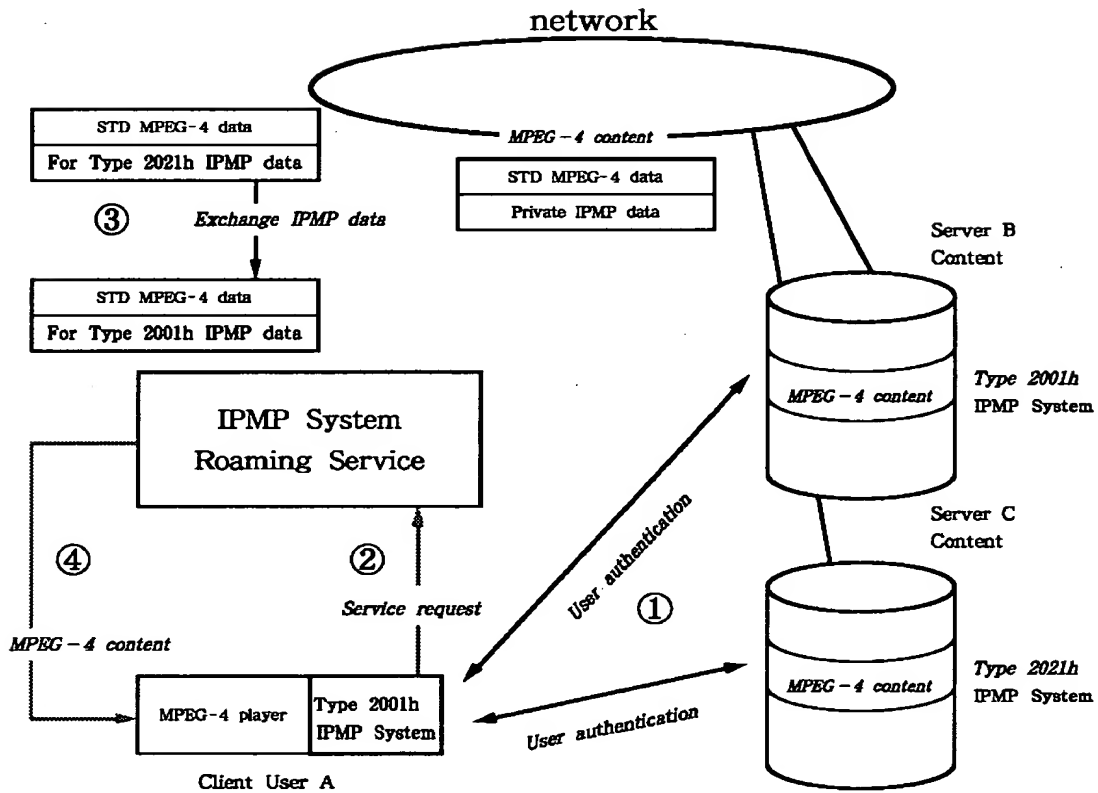


【図 1 3】

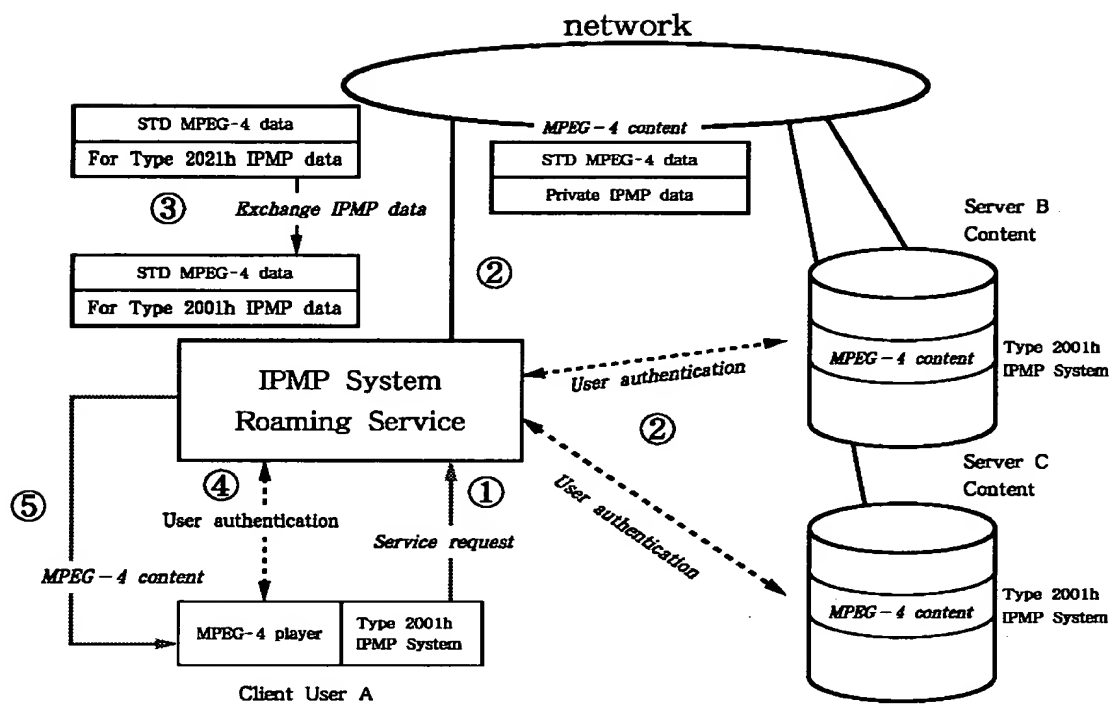
Case 2 : multi-path  
ex.OPIMA model



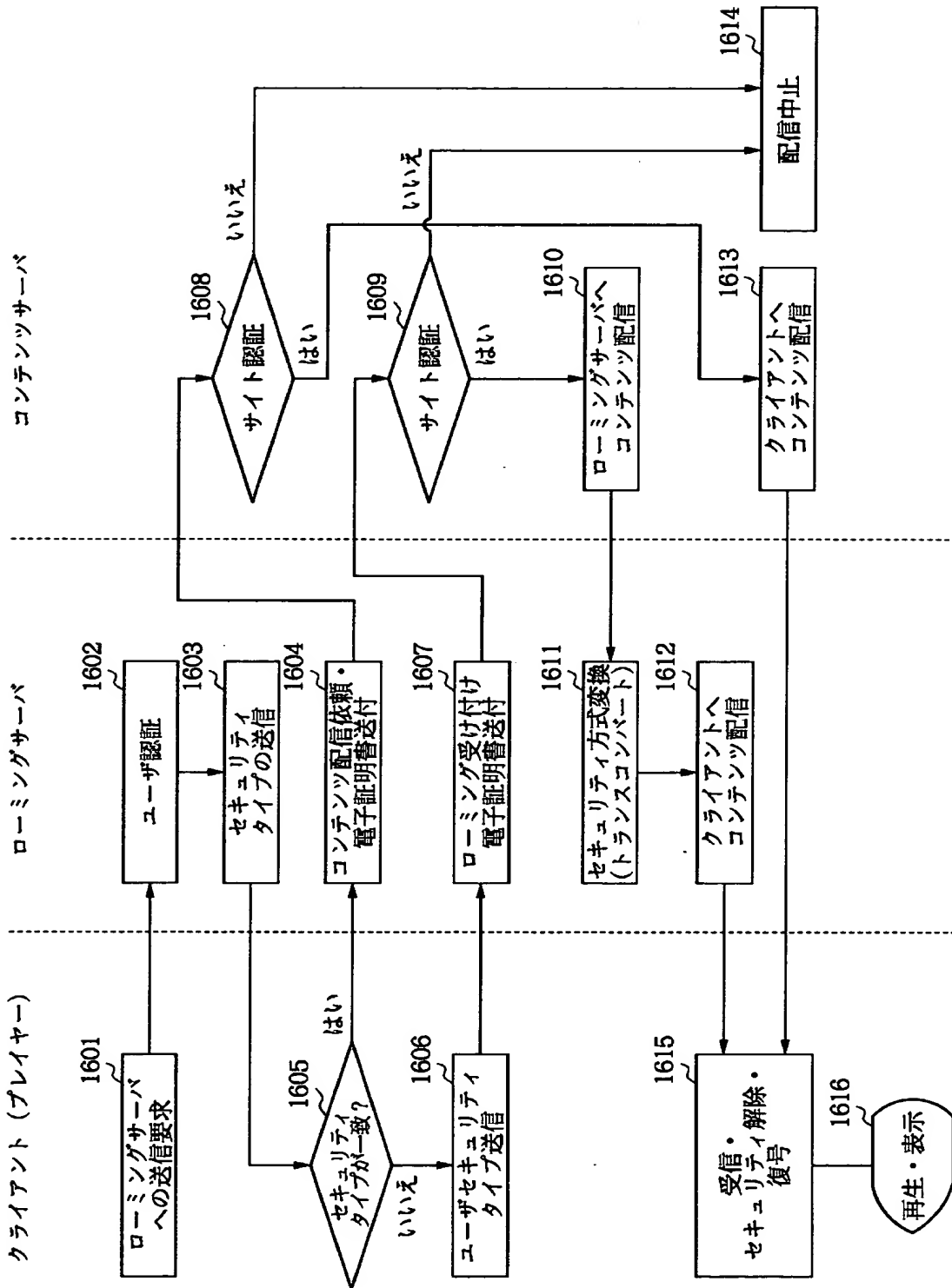
【図 14】



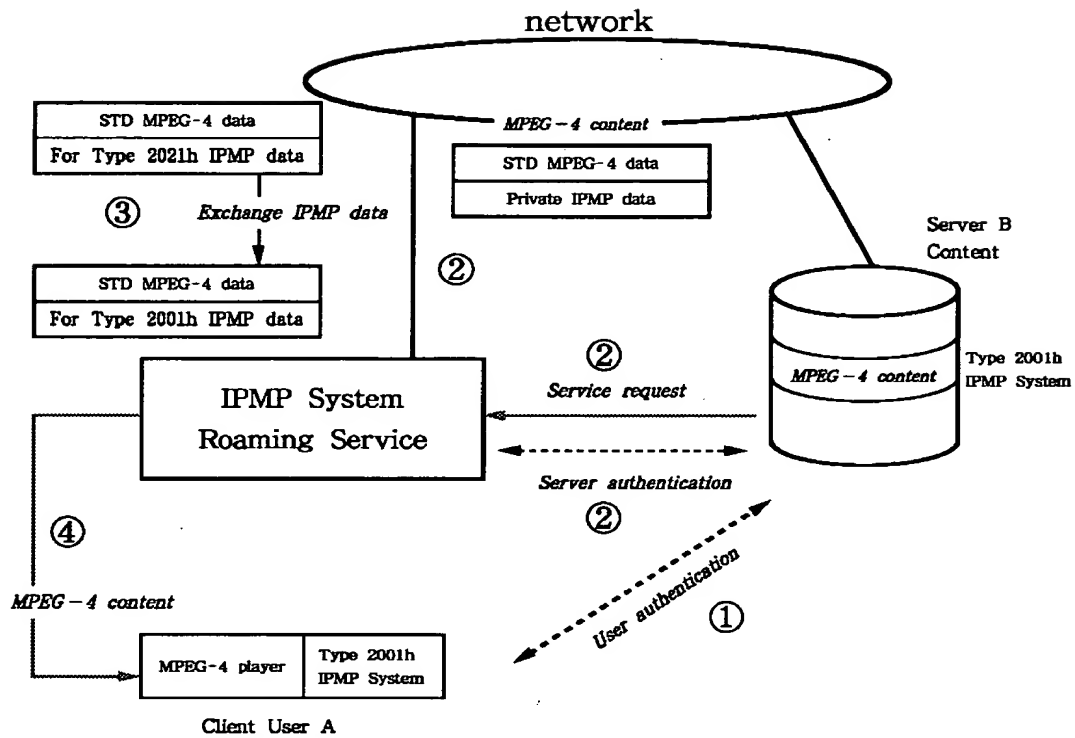
【図 1 5】



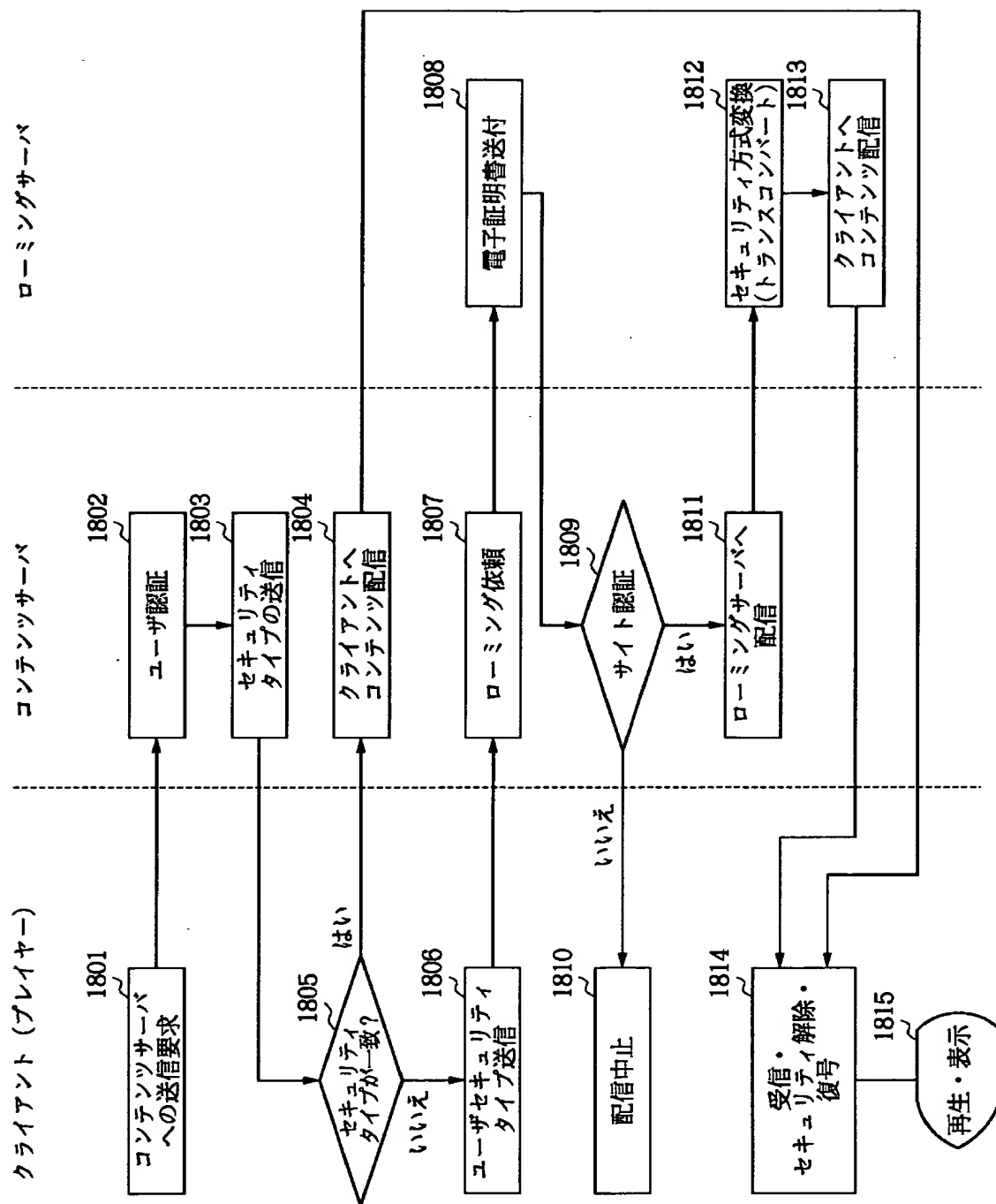
【図16】



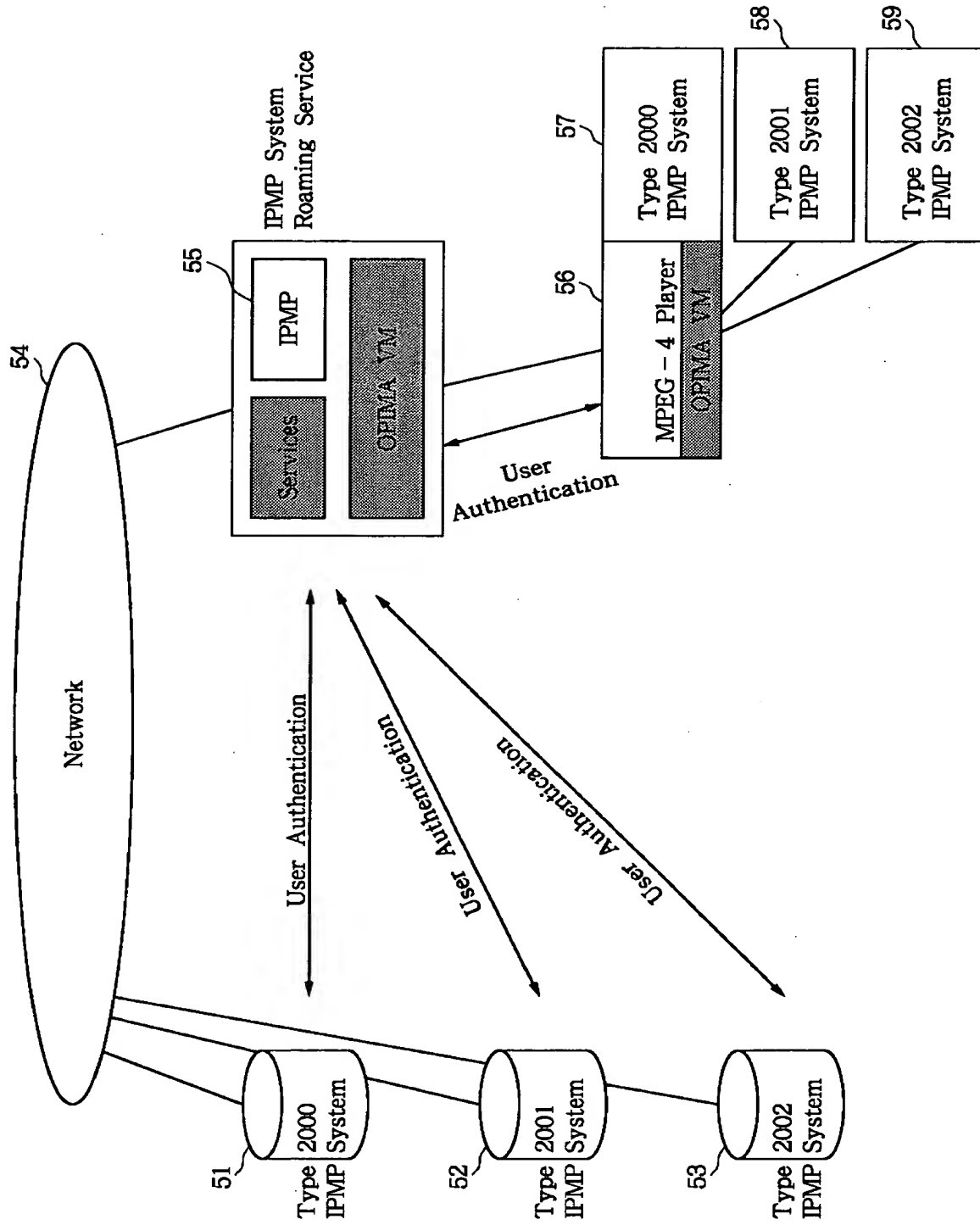
【図 1 7】



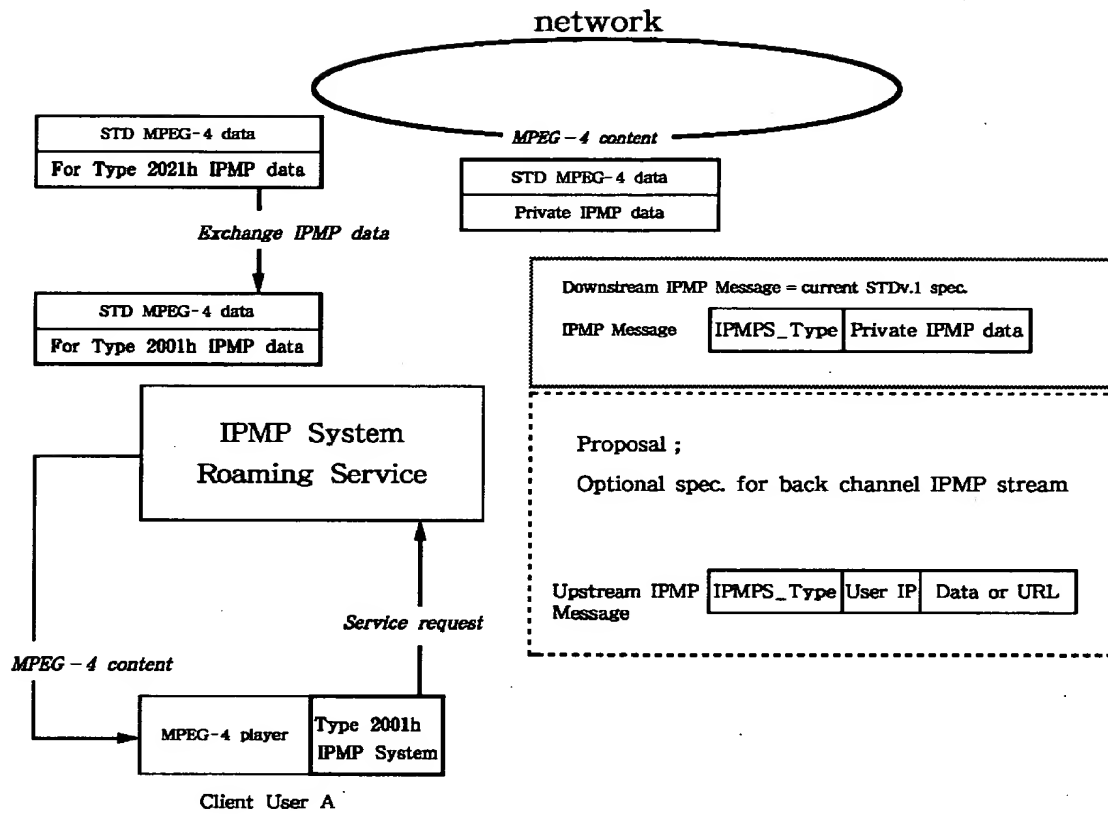
【図 18】



【図 1 9】

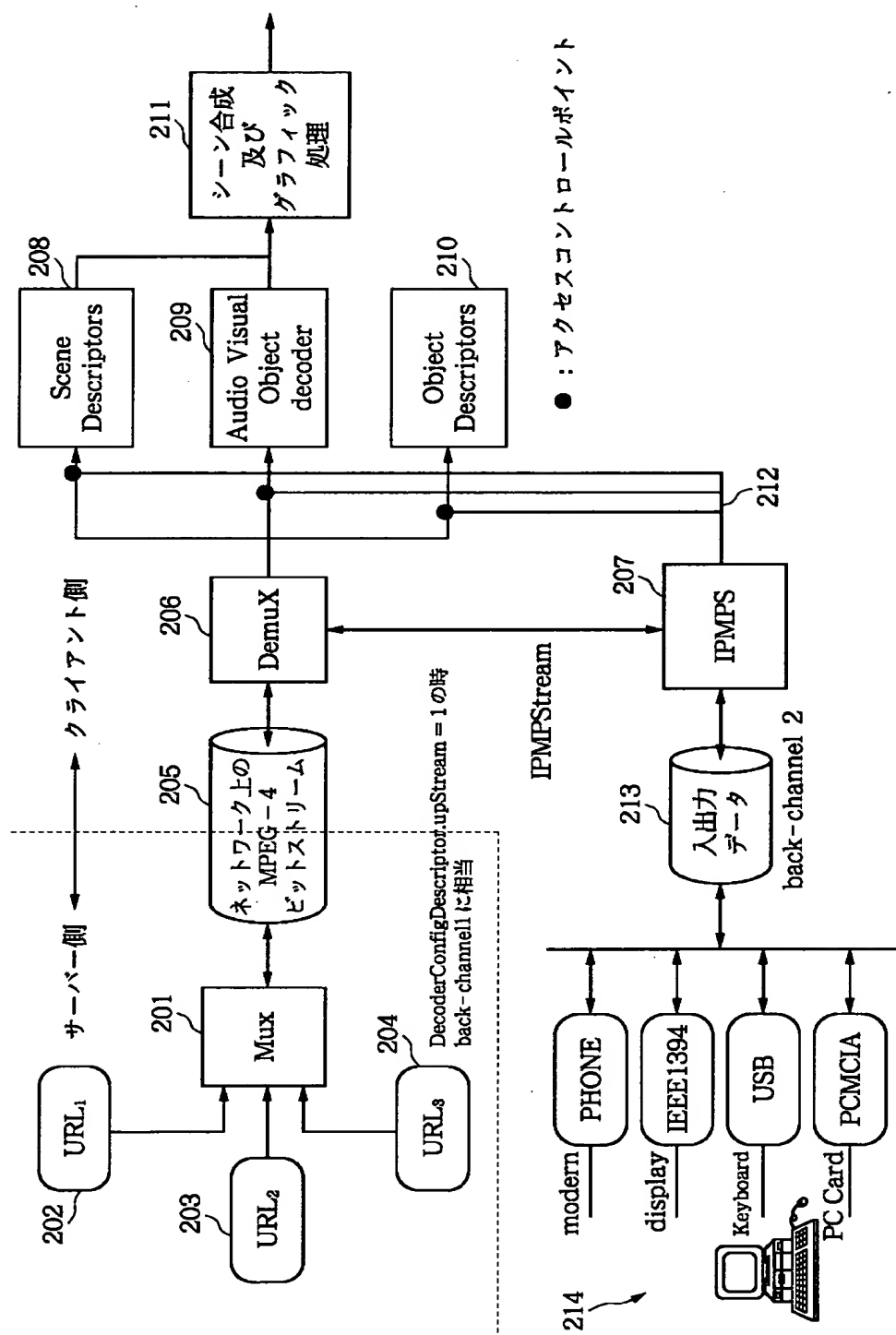


【図 2 0】

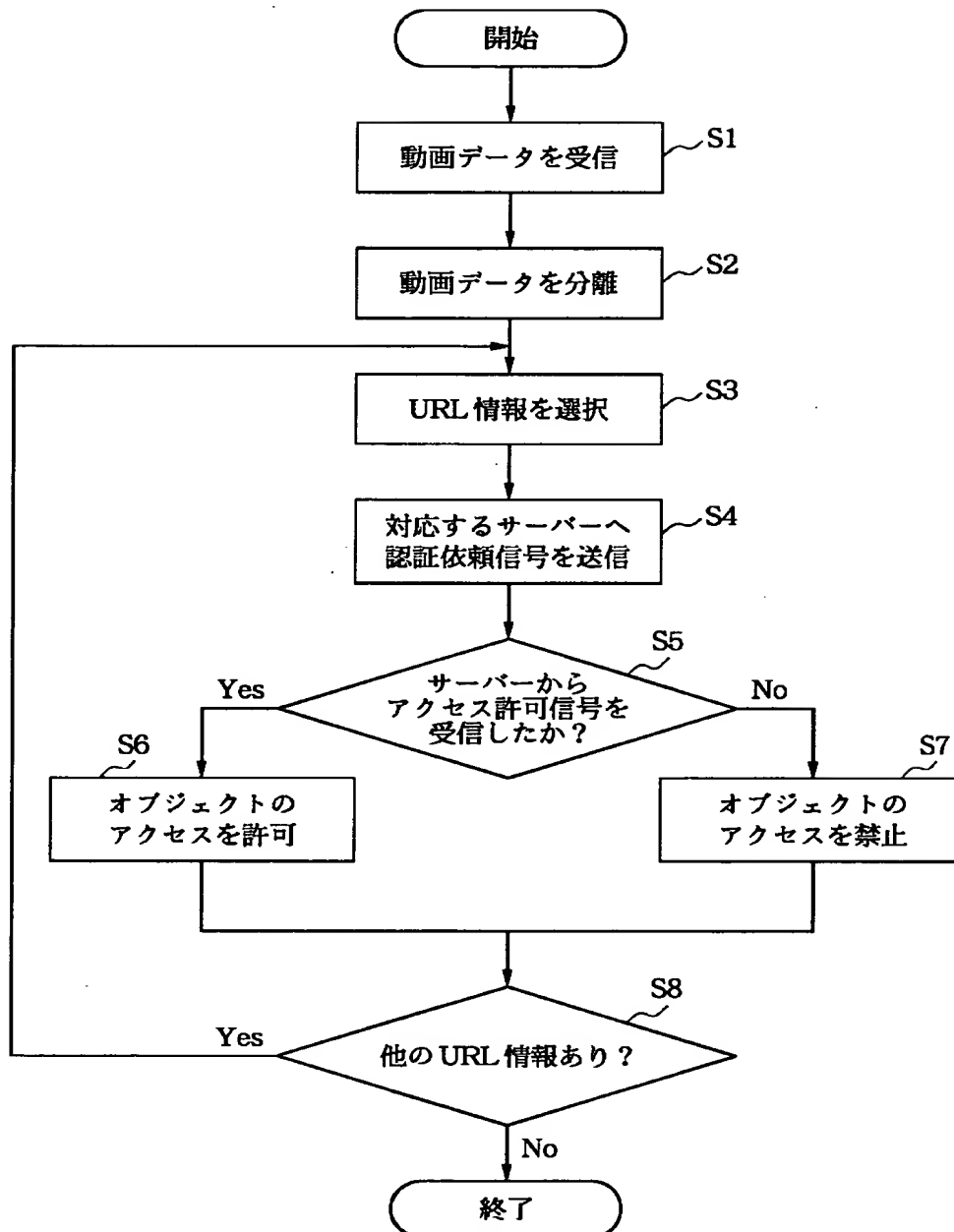




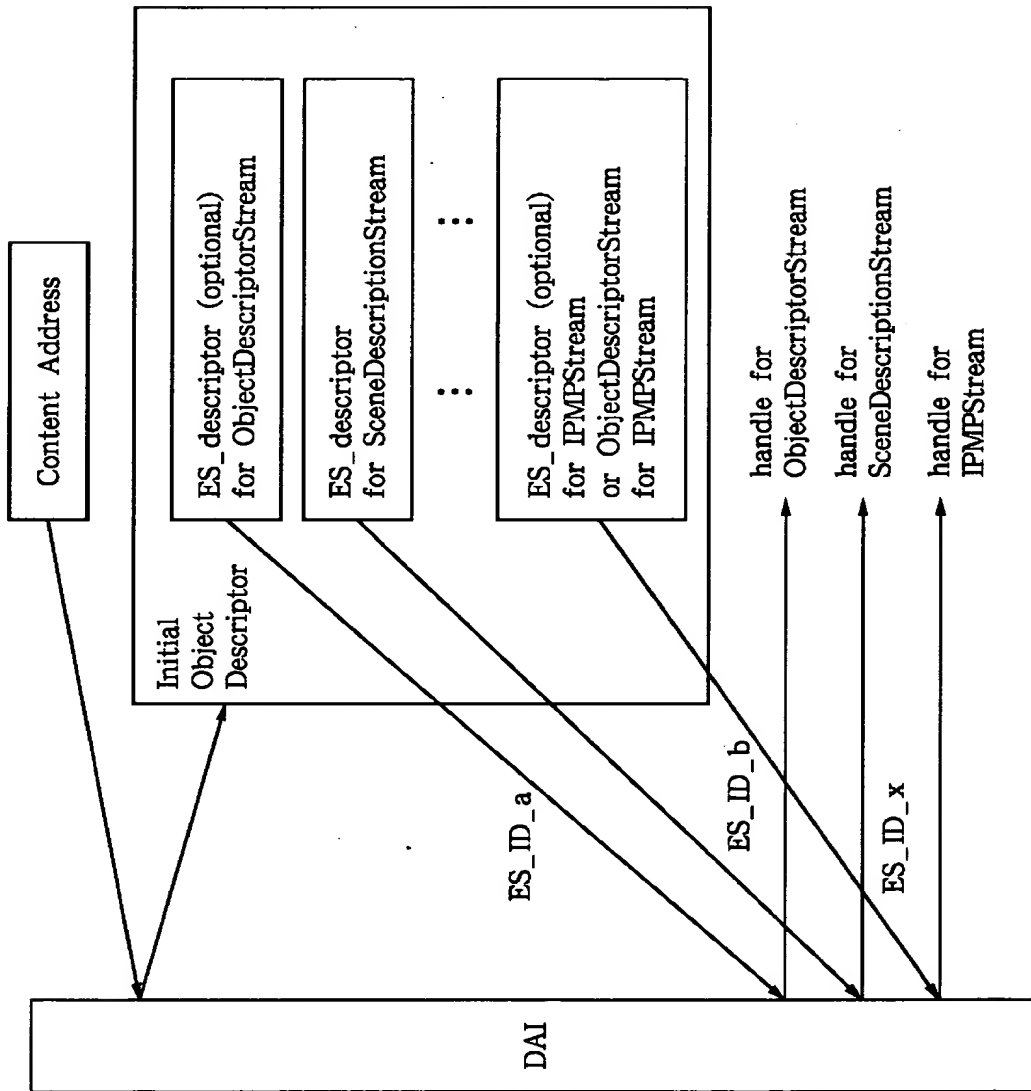
【図 21】



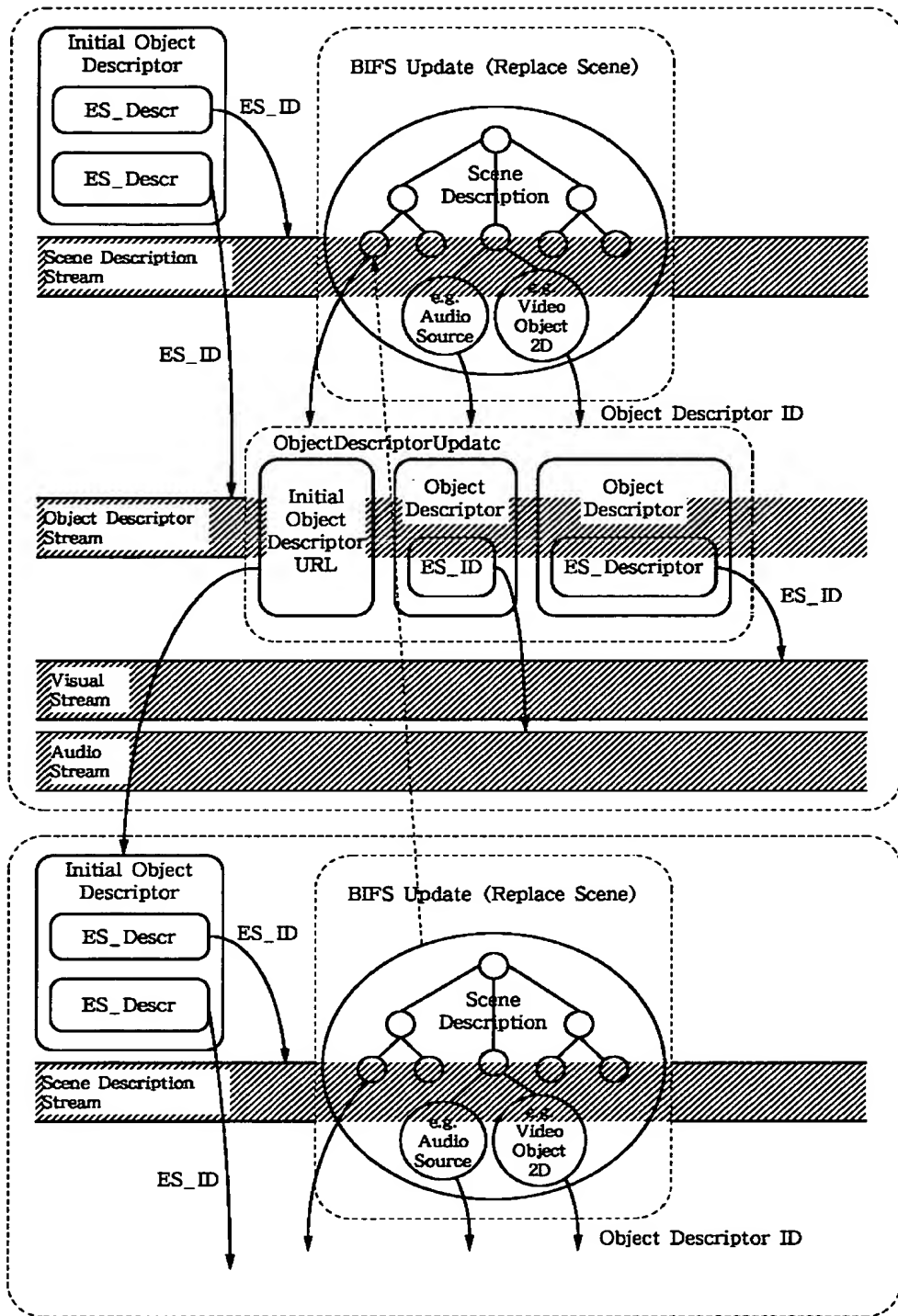
【図 2 2】



【図 23】



【図 24】



【書類名】 要約書

【要約】

【課題】 様々な知的財産保護システムを施されたデジタルコンテンツの再生をシン・クライアントで達成できるデジタルコンテンツ配信システムを提供する。

【解決手段】 クライアント、デジタルコンテンツサーバ、ローミングサーバ及びこれらの間を接続するネットワークを有して構成されるデジタルコンテンツ配信システムにおいて、前記ローミングサーバは、デジタルコンテンツサーバから知的財産保護システムが施されたデジタルコンテンツを受信し、前記受信したデジタルコンテンツの知的財産保護システムを他の種類の知的財産保護システムに変換し、クライアントへ配信する。

【選択図】 図 1 5

出 願 人 履 歴 情 報

識別番号

[000001007]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都大田区下丸子3丁目30番2号

氏 名

キヤノン株式会社